Публичное акционерное общество
«ТНС энерго Нижний Новгород»
(ПАО «ТНС энерго НН»)

УТВЕРЖДЕНО
на заседании Совета директоров
ПАО «ТНС энерго НН»
Протокол № 15/349
от « 27 » декабря 2018 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Нижний Новгород
2018 год

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика разработана в соответствии с законодательством Российской Федерации и нормами права в части обеспечения информационной безопасности, требованиями нормативных актов Российской Федерации и основывается, в том числе, на Доктрине информационной безопасности Российской Федерации, утверждённой Указом Президента Российской Федерации от 05.12.2016 №646.

1.2. Настоящая Политика разработана в целях повышения эффективности и создания условия для обеспечения единой системы информационной безопасности ПАО «ТНС энерго НН» (далее – Общество), а также является документом, доступным любому работнику и пользователю его информационных ресурсов, представляет собой систему взглядов на проблему обеспечения информационной безопасности, устанавливает принципы построения системы управления информационной безопасностью на основе систематизированного изложения целей, процессов и процедур информационной безопасности.

1.3. Руководство Общества осознает важность и необходимость развития и совершенствования мер и средств обеспечения информационной безопасности в контексте развития законодательства и норм регулирования деятельности, а также развития реализуемых технологий. Соблюдение требований информационной безопасности позволит создать конкурентные преимущества Общества, обеспечить его финансовую стабильность, рентабельность, соответствие правовым, регулятивным и договорным требованиям и повышение имиджа.

1.4. Требования информационной безопасности соответствуют интересам (целям) деятельности Общества и предназначены для снижения рисков, связанных с информационной безопасностью, до приемлемого уровня. Факторы рисков в информационной сфере имеют отношение к его корпоративному управлению (менеджменту), организации и реализации бизнес-процессов, взаимоотношениям с контрагентами и клиентами, внутрихозяйственной деятельности. Факторы рисков в информационной сфере составляют значимую часть операционных рисков, а также имеют отношение и к иным рискам основной и управленческой деятельности.

1.5. Стратегия в области обеспечения информационной безопасности и защиты информации, наряду с прочим, включает выполнение в практической деятельности требований:

- российского законодательства в области безопасности, безопасности информационных технологий и защиты информации, безопасности персональных данных, коммерческой тайны и других правовых актов;
- нормативных актов федеральных органов исполнительной власти, уполномоченных в области обеспечения физической безопасности и технической защиты информации, противодействия техническим разведкам и обеспечения информационной безопасности и приватности;

1.6. Необходимые требования обеспечения информационной безопасности должны неукоснительно соблюдаться всеми работниками и другими сторонами как это определяется положениями внутренних нормативных документов Общества, а также требованиями договоров и соглашений, стороной которых является Общество.

1.7. Настоящая Политика распространяется на бизнес - процессы Общества и обязательна для применения его работниками и руководством, а также иными пользователями его информационных ресурсов.

1.8. Настоящая Политика является корпоративным документом по информационной безопасности первого уровня.

1.9. Документами, детализирующими положения корпоративной Политики применительно к одной или нескольким областям информационной безопасности, видам и технологиям деятельности Общества, являются Положение о защите информации, а также регламенты, которые являются документами по информационной безопасности второго уровня, оформляются как отдельные внутренние нормативные документы Общества, разрабатываются, согласовываются и утверждаются в соответствии с установленным в Обществе порядком.

2. СПИСОК ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ

Бизнес-процесс – последовательность технологически связанных операций по осуществлению конкретного вида деятельности Общества.

Информационная безопасность Общества (ИБ) – в настоящей Политике состояние защищенности технологических и бизнес - процессов Общества, объединяющих в своем составе работников Общества, технические и программные средства обработки информации, информацию в условиях угроз в информационной сфере.

Информационные системы и ресурсы Общества – совокупность программно-аппаратных комплексов Общества, применяемых для обеспечения бизнес - процессов Общества.

Инцидент информационной безопасности – это появление одного или нескольких нежелательных рисковых событий информационной безопасности, с которыми связана значительная вероятность нарушения конфиденциальности, целостности или доступности информационных активов и инфраструктуры и создания угрозы информационной безопасности.

ИТ-блок – совокупность самостоятельных структурных подразделений Общества, ответственных за развитие, эксплуатацию и сопровождение информационных систем.

Конфиденциальная информация (далее – КИ) – информация, в отношении которой Обществом установлен режим конфиденциальности, в том числе Коммерческая тайна Общества.

Модель угроз – описательное представление свойств или характеристик угроз безопасности информации.

Модель нарушителя – описательное представление опыта, знаний, доступных ресурсов возможных нарушителей ИБ, необходимых им для реализации угрозы ИБ, и возможной мотивации действий.

Ответственное подразделение – подразделение, отвечающее за корпоративную защиту. Основные функции в указанной сфере – внедрение настоящей Политики, разработка, внедрение и поддержка систем обеспечения информационной безопасности.

Пользователь информационной системы - физическое лицо, обладающее возможностью доступа к информационной системе Общества.

Режим конфиденциальности информации – организационно-технические мероприятия по защите информации, позволяющие обладателю КИ при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду, и реализующие меры по охране КИ.

Рисковое событие информационной безопасности – это событие, обусловленное операционным риском, повлекшее или способное повлечь за собой потери Общества и произошедшее по причине ошибочности или сбоя производственных процессов, действий людей и систем, а также по причине внешних событий.

Угроза информационной безопасности – операционный риск, влияющий на нарушение одного (или нескольких) свойств информации – целостности, конфиденциальности, доступности объектов защиты.

3. ОПИСАНИЕ ОБЪЕКТА ЗАЩИТЫ

3.1. Основными объектами защиты системы информационной безопасности в Обществе являются:

- информационные ресурсы, содержащие коммерческую тайну, конфиденциальную информацию, включая персональные данные физических лиц, сведения ограниченного распространения, а также открыто распространяемая информация, необходимая для работы Общества, независимо от формы и вида ее представления;
- работники Общества, являющиеся разработчиками и пользователями информационных систем Общества;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства

защиты информации, объекты и помещения, в которых размещены такие системы.

4. ЦЕЛИ И ЗАДАЧИ ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Целью деятельности по обеспечению информационной безопасности Общества является снижение угроз информационной безопасности до приемлемого для Общества уровня.

4.2. Основные задачи деятельности по обеспечению информационной безопасности Общества:

- выявление потенциальных угроз информационной безопасности и уязвимостей объектов защиты;
- предотвращение инцидентов информационной безопасности;
- исключение либо минимизация выявленных угроз.

5. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Все множество потенциальных угроз безопасности информации делится на три класса по природе их возникновения: антропогенные, техногенные и естественные (природные).

5.1. Возникновение антропогенных угроз обусловлено деятельностью человека. Среди них можно выделить угрозы, возникающие вследствие как непреднамеренных (неумышленных) действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т.п., так и угрозы, возникающие в силу умышленных действий, связанные с корыстными, идейными или иными устремлениями людей.

5.2. Возникновение техногенных угроз обусловлено воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, не обусловленных напрямую деятельностью человека.

К техногенным угрозам могут быть отнесены сбои, в том числе в работе, или разрушение систем, созданных человеком.

5.3. Возникновение естественных (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

К естественным (природным) угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные и пр., включая экстремальные климатические условия, метеорологические явления, стихийные бедствия.

5.4. Источники угроз по отношению к инфраструктуре Общества могут быть как внешними, так и внутренними.

6. МОДЕЛЬ НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. По отношению к Обществу нарушители могут быть разделены на внешних и внутренних нарушителей:

6.1.1. В качестве потенциальных внутренних нарушителей Обществом рассматриваются:

- зарегистрированные пользователи информационных систем Общества;
- работники Общества, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам информационных систем Общества, но имеющие доступ в здания и помещения;
- персонал, обслуживающий технические средства корпоративной информационной системы Общества;
- работники самостоятельных структурных подразделений Общества, задействованные в разработке и сопровождении программного обеспечения;

- работники самостоятельных структурных подразделений, обеспечивающие безопасность Общества;

- руководители различных уровней.

6.1.2.В качестве потенциальных внешних нарушителей Обществом рассматриваются:

- бывшие работники Общества;

- представители организаций, взаимодействующих по вопросам технического обеспечения Общества;

- клиенты Общества;

- посетители зданий и помещений Общества;

- конкурирующие с Обществом организации;

- члены преступных организаций, сотрудники спецслужб или лица, действующие по их заданию;

- лица, случайно или умышленно проникшие в корпоративную информационную систему Общества из внешних телекоммуникационных сетей (хакеры).

6.2. В отношении внутренних и внешних нарушителей принимаются следующие ограничения и предположения о характере их возможных действий:

- нарушитель скрывает свои несанкционированные действия от других работников Общества;

- несанкционированные действия нарушителя могут быть следствием ошибок пользователей, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;

- в своей деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и информационные системы, адекватные финансовые средства для подкупа персонала, шантаж, методы социальной инженерии и другие средства и методы для достижения стоящих перед ним целей;

- внешний нарушитель может действовать в сговоре с внутренним нарушителем.

7. ОСНОВНЫЕ ПОЛОЖЕНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

7.1. Требования об обеспечении информационной безопасности Общества обязательны к соблюдению всеми работниками Общества и пользователями информационных систем.

7.2.Руководство Общества приветствует и поощряет в установленном порядке деятельность работников Общества и пользователей информационных систем по обеспечению информационной безопасности.

7.3.Неисполнение или некачественное исполнение работниками Общества и пользователей информационных систем обязанностей по обеспечению информационной безопасности может повлечь лишение доступа к информационным системам, а также применение к виновным дисциплинарных мер воздействия, степень которых определяется установленным в Обществе порядком либо требованиями действующего законодательства.

7.4. Стратегия Общества в части противодействия угрозам информационной безопасности заключается в сбалансированной реализации взаимодополняющих мер по обеспечению безопасности: от организационных мер на уровне руководства Общества, до специализированных мер информационной безопасности по каждому выявленному в Обществе риску, основанных на оценке рисков информационной безопасности.

7.5. С целью поддержки заданного уровня защищенности Общество придерживается процессного подхода в построении системы менеджмента информационной безопасности.

7.5.1. Система менеджмента информационной безопасности Общества основывается на осуществлении следующих основных процессов: планирование, реализация и эксплуатация защитных мер, проверка (мониторинг и анализ), совершенствование.

Реализация этих процессов осуществляется в виде непрерывного цикла – «планирование – реализация – проверка – совершенствование – планирование – …», направленного на постоянное совершенствование деятельности по обеспечению информационной безопасности Общества и повышение ее эффективности.

7.5.2. На всех этапах жизненного цикла управление информационной безопасностью Общества осуществляется с соблюдением нормативных документов, определяющих

процессы управления операционными рисками Общества.

7.6. При планировании мероприятий по обеспечению информационной безопасности в Обществе осуществляются:

7.6.1. Определение и распределение ролей персонала Общества, связанного с обеспечением информационной безопасности (ролей информационной безопасности).

7.6.2. Оценка важности информационных активов с учетом потребности в обеспечении их свойств с точки зрения информационной безопасности.

7.6.3. Менеджмент рисков информационной безопасности, включающий:

- анализ влияния на информационную безопасность Общества применяемых в деятельности Общества технологий, а также внешних по отношению к Обществу событий;
- выявление проблем обеспечения информационной безопасности, анализ причин их возникновения и прогнозирование их развития;
- определение моделей угроз информационной безопасности;
- выявление, анализ и оценка значимых для Общества угроз информационной безопасности;
- выявление возможных негативных последствий для Общества, наступающих в результате проявления факторов риска информационной безопасности, в том числе связанных с нарушением свойств безопасности информационных активов Общества;
- идентификацию и анализ рисковых событий информационной безопасности;
- оценку величины рисков информационной безопасности и определение среди них рисков, неприемлемых для Общества;
- обработку результатов оценки рисков информационной безопасности, базирующейся на методах управления операционными рисками, определенных в Обществе;
- оптимизацию рисков информационной безопасности за счет выбора и применения защитных мер, противодействующих проявлениям факторов риска и минимизирующих возможные негативные последствия для Общества в случае наступления рисковых событий;
- оценку влияния защитных мер на цели основной деятельности Общества;
- оценку затрат на реализацию защитных мер;
- рассмотрение и оценку различных вариантов решения задач по обеспечению информационной безопасности;
- разработку планов управления рисками, предусматривающих различные защитные меры и варианты их применения, и выбор из них такого, реализация которого максимально положительно скажется на целях основной деятельности Общества и будет оптимальна с точки зрения произведенных затрат и ожидаемого эффекта;
- документальное оформление целей и задач обеспечения информационной безопасности Общества, поддержка в актуальном состоянии нормативно – методического обеспечения деятельности в сфере информационной безопасности.

7.7. В рамках реализации деятельности по обеспечению информационной безопасности в Обществе осуществляются:

7.7.1. Менеджмент инцидентов информационной безопасности, включающий:

- сбор информации о событиях информационной безопасности;
- выявление и анализ инцидентов информационной безопасности;
- расследование инцидентов информационной безопасности;
- оперативное реагирование на инцидент информационной безопасности;
- минимизация негативных последствий инцидентов информационной безопасности;
- оперативное доведение до руководства Общества информации по наиболее значимым инцидентам информационной безопасности и оперативное принятие решений по ним, включая регламентирование порядка реагирования на инциденты информационной безопасности;
- выполнение принятых решений по всем инцидентам информационной безопасности в установленные сроки;
- пересмотр применяемых требований, мер и механизмов по обеспечению информационной безопасности по результатам рассмотрения инцидентов информационной безопасности;
- повышение уровня знаний персонала Общества в вопросах обеспечения информационной безопасности;
- обеспечение регламентации и управления доступом к программным и программно-

техническим средствам и сервисам автоматизированных систем Общества и информации, обрабатываемой в них;

- применение сертифицированных средств криптографической защиты информации;
- обеспечение бесперебойной работы автоматизированных систем и сетей связи;
- обеспечение возобновления работы автоматизированных систем и сетей связи после прерываний и нештатных ситуаций;
- применение средств защиты от вредоносных программ;
- обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных систем Общества, связанных с проектированием, разработкой, приобретением, поставкой, вводом в действие, сопровождением (сервисным обслуживанием);
- обеспечение информационной безопасности при использовании доступа в сеть Интернет и услуг электронной почты;
- контроль доступа в здания и помещения Общества.

7.7.2. Обеспечение защиты информации от утечки по техническим каналам, включающее:

- применение мер и технических средств, снижающих вероятность несанкционированного получения информации в устной форме - пассивная защита;
- применение мер и технических средств, создающих помехи при несанкционированном получении информации - активная защита;
- применение мер и технических средств, позволяющих выявлять каналы несанкционированного получения информации - поиск.

7.8. В целях проверки деятельности по обеспечению информационной безопасности в Обществе осуществляются:

- контроль правильности реализации и эксплуатации защитных мер;
- контроль изменений конфигурации систем и подсистем Общества;
- мониторинг факторов рисков и соответствующий их пересмотр;
- контроль реализации и исполнения требований работниками Общества действующих внутренних нормативных документов по обеспечению информационной безопасности Общества;
- контроль деятельности работников и других пользователей информационных систем Общества, направленный на выявление и предотвращение конфликтов интересов.

7.9. В целях совершенствования деятельности по обеспечению информационной безопасности в Обществе осуществляется периодическое, а при необходимости оперативное, уточнение/пересмотр целей и задач обеспечения информационной безопасности (при изменениях целей и задач основной деятельности Общества).

8. ОРГАНИЗАЦИОННАЯ ОСНОВА ДЕЯТЕЛЬНОСТИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

8.1. В целях выполнения задач по обеспечению информационной безопасности Общества, в соответствии с рекомендациями международных и российских стандартов по безопасности в Обществе должны быть определены следующие роли:

- Координатор (Заместитель Генерального директора по правовой защите и экономической безопасности ПАО ГК «ТНС энерго», Дирекция экономической безопасности ПАО ГК «ТНС энерго»);
- Ответственное подразделение (подразделение, отвечающее за корпоративную защиту, соисполнитель – ИТ-блок);
- Работник Общества.

При необходимости могут быть определены и другие роли по информационной безопасности.

8.2. Основными функциями Координатора в вопросах информационной безопасности являются:

- координация и внедрение положений Политики информационной безопасности в Обществе;
- общее руководство и контроль за обеспечением информационной безопасности Общества;

- согласование ответственных лиц в области ИБ.

8.3. Оперативная деятельность и планирование деятельности по обеспечению информационной безопасности Общества осуществляются и координируются Ответственным подразделением. Задачами Ответственного подразделения являются:

8.3.1. установление потребностей Общества в применении мер обеспечения информационной безопасности, определяемых как внутренними корпоративными требованиями, так и требованиями нормативных актов;

8.3.2. соблюдение действующего федерального законодательства, нормативных актов федеральных органов исполнительной власти, уполномоченных в области обеспечения безопасности и противодействия техническим разведкам и технической защиты информации;

8.3.3. разработка и пересмотр внутренних нормативных документов по обеспечению информационной безопасности Общества, включая планы, политики, положения, регламенты, инструкции, методики, перечни сведений и иные виды внутренних нормативных документов;

8.3.4. осуществление контроля актуальности и непротиворечивости внутренних нормативных документов (политик, планов, методик и т.д.), затрагивающих вопросы информационной безопасности Общества;

8.3.5. обучение, контроль и непосредственная работа с работниками Общества в области обеспечения информационной безопасности;

8.3.6. планирование применения, участие в организации поставки и эксплуатации средств обеспечения информационной безопасности на объекты и системы в Обществе;

8.3.7. выявление и предотвращение реализации угроз информационной безопасности;

8.3.8. выявление и реагирование на инциденты информационной безопасности;

8.3.9. прогнозирование и предупреждение инцидентов информационной безопасности;

8.3.10. пресечение несанкционированных действий нарушителей информационной безопасности;

8.3.11. поддержка базы инцидентов информационной безопасности, анализ, разработка оптимальных процедур реагирования на инциденты и обучение работников;

8.3.12. типизация решений по применению мер и средств обеспечения информационной безопасности;

8.3.13. обеспечение эксплуатации средств и механизмов обеспечения информационной безопасности;

8.3.14. мониторинг и оценка информационной безопасности, включая оценку полноты и достаточности защитных мер и видов деятельности по обеспечению информационной безопасности Общества;

8.3.15. контроль обеспечения информационной безопасности Общества, в том числе, и на основе информации об инцидентах информационной безопасности, результатах мониторинга, оценки и аудита информационной безопасности;

8.3.16. информирование руководства Общества и руководителей его структурных подразделений Общества об угрозах информационной безопасности, влияющих на деятельность Общества.

8.4. Ответственное подразделение Общества может создавать комиссии для проведения расследований инцидентов информационной безопасности, и может, при наличии обоснованной необходимости по согласованию с руководителями соответствующих подразделений, привлекать для работы в них работников других самостоятельных структурных подразделений на основе совмещения работы в комиссии со своими основными должностными обязанностями. Порядок создания комиссии и принятия ею решений определяется локальным нормативным актом Общества.

О наиболее значимых инцидентах Ответственное подразделение незамедлительно докладывает Координатору.

8.5. Финансирование работ по реализации положений настоящей Политики осуществляется как в рамках целевого бюджета Ответственного подразделения Общества, так и в рамках бюджетов бизнес - подразделений и подразделений ИТ-блока.

8.6. Основными задачами работников Общества при выполнении возложенных на них обязанностей и в рамках их участия в деятельности по обеспечению информационной безопасности Общества являются:

- соблюдение требований информационной безопасности, устанавливаемых

нормативными документами Общества;

- реагирование на инциденты информационной безопасности;
- прогнозирование и предупреждение инцидентов информационной безопасности в пределах своей компетенции;
- мониторинг и оценка информационной безопасности в рамках своего участка работы (рабочего места, структурного подразделения) и в пределах своей компетенции;
- информирование своего руководства и Ответственного подразделения о выявленном инциденте информационной безопасности, либо об угрозе его возникновения в информационной среде Общества.

9. ОТВЕТСТВЕННОСТЬ ЗА СОБЛЮДЕНИЕ ПОЛОЖЕНИЙ ПОЛИТИКИ

9.1. Ответственность за координацию, внедрение и внесение изменений в настоящую Политику несет Координатор.

9.2. Ответственность за поддержание положений настоящей Политики в актуальном состоянии, организацию координации, внедрения, и внесение изменений в процессы системы менеджмента информационной безопасности Общества возлагается на руководство Ответственного подразделения.

9.3. Ответственность работников Общества за невыполнение настоящей Политики определяется соответствующими положениями, включаемыми в трудовые договоры с работниками Общества, а также положениями внутренних нормативных документов Общества.

10. КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ ПОЛОЖЕНИЙ ПОЛИТИКИ

10.1. Общий контроль состояния информационной безопасности осуществляется Координатором.

10.2. Текущий контроль соблюдения настоящей Политики осуществляет Ответственное подразделение.

10.3. Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов информационной безопасности Общества, по результатам оценки информационной безопасности, а также в рамках иных контрольных мероприятий.

11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

11.1. Требования настоящей Политики могут быть дополнены и уточнены другими внутренними нормативными документами Общества.

11.2. В случае изменения действующего законодательства и иных нормативных актов, а также Устава Общества настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также Уставу Общества. В этом случае Ответственное подразделение обязано незамедлительно инициировать внесение соответствующих изменений.

11.3. Внесение изменений в настоящую Политику осуществляется на периодической и внеплановой основе:

- периодическое внесение изменений в настоящую Политику должно осуществляться для отражения изменений законодательства и нормативных актов, отраслевых принципов и технических регламентов;
- внеплановое внесение изменений в настоящую Политику может производиться по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности, результатам проведения внутренних аудитов информационной безопасности и других контрольных мероприятий.