Процедура
Интегрированной Системы Управления

ПР 12-05

УТВЕРЖДЕНО:
Директор
ООО «АГРОПРОСПЕРИС»

И.В.Осьмачко

Политика информационной безопасности

Редакция
2-2019

Оглавление

1. НАЗНАЧЕНИЕ И ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Политика информационной безопасности (далее - Политика) определяет совокупность правил, требований и руководящих принципов в области информационной безопасности, которыми руководствуется Группа компаний «Агропросперис» (далее – Группа) в своей деятельности, а также определяет основные принципы и задачи системы управления информационной безопасностью (далее - СУИБ).

1.2. Политика является нормативной основой для защиты информационных активов Группы в целях обеспечения:

- конфиденциальности - обеспечения доступности к информации, информационным системам и иным программным процессам только для авторизованных пользователей, которым предоставлены на то соответствующие полномочия в минимально необходимом объеме;

- целостности - защиты точности, корректности и полноты информации и методов её обработки;

- доступности - означает, что имеющий соответствующие полномочия авторизованный пользователь или процесс может в любое время без особых проблем получить доступ к информационным системам Группы;

- наблюдаемости – обеспечения возможности мониторинга действий пользователей, процессов, работающих с информационными активами Группы, времени и даты такой работы, а также обеспечения принципа невозможности отказа от выполненных действий.

1.3. Политика основана на требованиях международных стандартов в области информационной безопасности.

1.4. Настоящая Политика является документом по информационной безопасности первого уровня. Документы второго уровня являются детализацией данной Политики по конкретным направлениям и вопросам (Положения, Правила, Инструкции и т.д.).

1.5. Настоящая Политика обязательна для применения во всех Компаниях Группы и ознакомления всеми сотрудниками и руководством Субъектов Группы.

2. НОРМАТИВНЫЕ ССЫЛКИ

2.1. Политика разработана в соответствии с международным стандартом ISO/IEK 27001:2013 “Информационные технологии – Методы защиты – Системы менеджмента информационной безопасности - Требования”.

3. ТЕРМИНЫ

3.1. В целях единообразного понимания и надлежащего исполнения данной Политики термины, определения, аббревиатуры, условные обозначения и сокращения имеют следующее значения (если в тексте Политики прямо не оговорено иное):

Безопасность информации - защищенность информации от несанкционированного и/или нежелательного ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

Информационные активы – информация в любом её виде, носители информации, информационные системы, телекоммуникационные сети, программное обеспечение в любой форме его получения (приобретенное или собственной разработки), в отношении которой необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации.

Авторизованный пользователь – сотрудник Субъекта Группы или третье лицо, которые имеют полномочия использовать определенную информационную систему Группы, прошли регистрацию и находятся в системе под своим уникальным логином.

Угроза - реально или потенциально возможные действия по реализации опасных воздействующих факторов с целью преднамеренного или случайного (неумышленного) нарушения режима функционирования информационных систем и нарушения свойств защищаемой информации или других информационных активов.

Уязвимость – недостаток в информационной системе, программе, оборудовании, использование которого может приводить к нарушению целостности системы и некорректной ее работе. Уязвимости появляются в результате ошибок программирования, недостатков, которые допускались при проектировании системы, ненадежных паролей, вредоносных программ и т.п.

Риск ИБ – вероятность того, что определенная угроза может быть успешно реализована, что может нанести ущерб интересам Группы.

Нарушитель - лицо, которое предприняло (пыталось предпринять) попытку несанкционированного доступа к ресурсам системы (попытку выполнения запрещенных ему действий с данным ресурсом) по ошибке, незнанию или осознанно со злым умыслом (из корыстных или иных побуждений) или без такового (с целью самоутверждения и т.п.) и использовавшее для этого различные возможности, методы и средства.

Система управления информационной безопасностью (СУИБ) – часть общей системы управления Субъекта Группы, основанной на оценке рисков, которая создает, реализует, эксплуатирует, осуществляет мониторинг, пересмотр, сопровождение и совершенствование информационной безопасности.

Управление ИБ – циклический процесс, включающий осознание степени необходимости защиты информации и постановку задач; сбор и анализ данных о состоянии информационной безопасности в рамках Группы; оценку рисков ИБ; планирование мер по минимизации рисков; реализацию и внедрение соответствующих механизмов контроля, распределение ролей и ответственности, обучение персонала, оперативную работу по осуществлению защитных мероприятий; мониторинг функционирования механизмов контроля, оценку их эффективности и соответствующие корректирующие воздействия.

4. ОБЪЕКТЫ ЗАЩИТЫ

4.1. Основными объектами защиты системы информационной безопасности в Группе являются:

- территориально распределенная 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;

- информационные системы с ограниченным доступом, а также открытая (общедоступная) информация, необходимая для работы Группы, независимо от формы и вида ее предоставления;

- программное и аппаратное обеспечение бизнес-процессов Группы;

- процессы обработки информации в информационной системе, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей системы, а также ее обслуживающий персонал.

5. ОСНОВНЫЕ ПРИНЦИПЫ И ЦЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Основной целью системы информационной безопасности является защита корпоративных информационных систем Группы от возможного ущерба в результате случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки информации, хранения, передачи, а также минимизация соответствующих рисков.

5.2. Основными задачами деятельности по обеспечению ИБ Группы являются:

- прогнозирование и своевременное выявление угроз безопасности информационным активам Группы, причин и условий, способствующих нанесению ущерба, нарушению бизнес-процессов;

- создание условий функционирования Группы с наименьшей вероятностью реализации угроз безопасности информационным активам и нанесения им ущерба;

- выявление потенциальных угроз в сфере ИБ и уязвимостей объектов защиты;

- предотвращение инцидентов в сфере ИБ;

- создание механизмов и условий оперативного реагирования на угрозы в сфере ИБ и проявление негативных тенденций в функционировании информационных активов Группы;

- создание условий для максимально возможного возмещения и локализации ущерба, наносимого в результате инцидентов в сфере ИБ;

- повышение осведомленности сотрудников Группы, а в отдельных случаях - и третьих лиц, в области рисков, связанных с использованием информационных активов Группы, и их возможных последствий.

5.3. Построение системы управления информационной безопасности и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность (предполагает осуществление защитных мероприятий и разработку системы безопасности информации в соответствии с действующим законодательством Украины и международными стандартами безопасности);

- системность (при создании системы защиты должны учитываться все слабые и наиболее уязвимые места информационной системы, а также характер, возможные объекты и направления атак на нее со стороны нарушителей, пути проникновения в распределенные системы и несанкционированного доступа к информации);

- комплексность (комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз);

- непрерывность защиты (процесс обеспечения безопасности информации, который должен осуществляться на постоянной основе на всех уровнях внутри Группы, при этом каждый сотрудник Группы должен принимать участие в этом процессе);

- своевременность (предполагает упреждающий характер мер по обеспечению безопасности информации);

- совершенствование (предполагает постоянное совершенствование мер и средств защиты информации);

- разумная достаточность (предполагает соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения);

- персональная ответственность (в соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг лиц, причастных к такому нарушению, был четко известен или сведен к минимуму);

- минимизация полномочий (доступ к информации должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его трудовых обязанностей);

- гибкость системы защиты (система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления Группой своей деятельности);

- простота применения средств защиты (механизмы и методы защиты должны быть интуитивно понятны и просты в использовании);

- обязательность контроля (контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей).

5.4. В Группе используются следующие требования по обеспечению информационной безопасности:

- периодическая инвентаризация авторизованных и неавторизованных устройств в корпоративной сети;

- периодическая инвентаризация авторизованного и неавторизованного программного обеспечения серверов, рабочих станций;

- использование безопасных конфигураций для аппаратного, сетевого и программного обеспечения, ограничение и контроль сетевых портов;

- управление уязвимостями программного и аппаратного обеспечения, их своевременное устранение (patch management);

- разграничение и периодический контроль прав доступа пользователей;

- минимизация и контроль за использованием административных учетных записей;

- эффективная парольная защита;

- защита электронной почты и веб-браузера;

- защита от вредоносных программ;

- постоянный мониторинг и анализ системных журналов аудита работы на всех уровнях информационных систем;

- защита и контроль использования корпоративной сети;

- возможность восстановления данных;

- криптографическая защита информации.

6. РАЗДЕЛЕНИЕ ПОЛНОМОЧИЙ И ОТВЕТСТВЕННОСТИ

6.1. Руководство Группы осуществляет координацию деятельности всех подразделений для организации процессов информационной безопасности.

6.2. В рамках исполнения настоящей Политики проводится регулярный мониторинг и аудит информационных систем.

6.3. Руководители Субъектов Группы и их структурных подразделений несут ответственность за ознакомление сотрудников с требованиями данной Политики.

6.4. Администраторы информационных систем обеспечивают непрерывное функционирование всех элементов автоматизированных систем и процессов, а также отвечают за реализацию мер, необходимых для реализации данной Политики.

6.5. Каждый сотрудник несет ответственность за соблюдение требований, определенных данной Политикой, иных действующих в рамках Группы правил, инструкций, рекомендаций и прочих внутренних документов по обеспечению информационной безопасности, а также за своевременное извещение непосредственного руководства обо всех подозрительных ситуациях и возможных инцидентах.

6.6. За нарушение данной Политики, могут применяться меры, предусмотренные трудовым законодательством.

7. ПЕРЕСМОТР ДОКУМЕНТА

7.1. Политика пересматривается по мере необходимости при появлении и/или изменении информационных активов Группы и/или новых технологий, а также в случае изменения законодательных и иных норм и требований.