ТОО «Automation Technology and Solutions»
ИИН: KZ 95998 BTB 0000 1244 76 KZT
БИН: 120 540 011 136
Свидетельство о гос. Регистрации:
43168-1907-ТОО от 17 мая 2012
010000, Республика Казахстан, г. Астана, район Алматы, Юго-Восток, ул. Ер Таргын, д. 27
АО «Цеснабанк»
БИК: TSES KZ KA
Код: 17 КБЕ
телефон: 8(717) 262 54 88
E-mail: info@atsolut.kz
www.atsolut.kz

ЖШС «Automation Technology and Solutions»
ЖСК: KZ 95998 BTB 0000 1244 76 KZT
БСН: 120 540 011 136
Мемлекеттік тіркелу туралы куәлік:
43168-1907-ТОО, 17 Мамыр 2012 ж.
010000, Қазақстан Республикасы, Астана қ., Алматы ауданы, Юго-Восток тұрғын алабы, Ер Тарғын көшесі, 27 үй,
АҚ «ЦЕСНАБАНК»
БСК: TSES KZ KA
Код: 17 КБЕ
телефон: 8(717) 262 54 88
E-mail: info@atsolut.kz
www.atsolut.kz

Инструкция

«О мерах по обеспечению информационной безопасности»

1. Общие положения

Инструкция устанавливает порядок организации и правила обеспечения информационной безопасности в ТОО «Automation Technology Solutions» (далее по тексту – ТОО), распределение функций и ответственности за обеспечение информационной безопасности между подразделениями и сотрудниками, требования по информационной безопасности к используемым средствам информатизации.

Действие Инструкции распространяется на области деятельности ТОО, в которых для работы с информацией применяются различного рода технические средства.

Основные термины и определения:

- безопасность информации - состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования информации и т.п.

- доступ к информации – комплекс организационно-технических мероприятий, позволяющих сотруднику получить возможность ознакомления с информацией, в том числе с помощью технических средств, в соответствии с предоставленными ему для этого правами;

- защита информации – комплекс организационно-технических мероприятий, направленных на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;

- защита информации от непреднамеренного воздействия - деятельность, направленная на предотвращение воздействия на защищаемую информацию ошибок её пользователя, сбоя технических и программных средств информационных систем, природных явлений или иных нецеленаправленных на изменение информации мероприятий, приводящих к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

- защита информации от несанкционированного воздействия - деятельность, направленная на предотвращение воздействия на защищаемую информацию с нарушением установленных прав и(или) правил на изменение информации, приводящего к её искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

- защита информации от несанкционированного доступа - деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами и собственником (ТОО) прав или правил доступа к защищаемой информации;

- информация – сведения о лицах, предметах, событиях, явлениях и процессах (независимо от формы их представления), используемые в целях принятия решений;

- информация ТОО – информация, принадлежащая ТОО, то есть:
    - созданная самим ТОО (его сотрудниками) в процессе его деятельности;
    - приобретенная ТОО, а законных основаниях;
    - переданная ТОО его партнерами (клиентами) при установлении сотрудничества на правах совместного владения;
    - полученная в результате целенаправленного сбора информации подразделениями ТОО;

- информационная безопасность – состояние защищённости информационной среды, обеспечивающее минимизацию ущерба, вызванного возможной утечкой защищаемой информации, а также несанкционированных и непреднамеренных воздействий;

- информационная система – организационно-упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием вычислительной техники;

- информационная сфера (среда) - совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений;

- конфиденциальная информация – документированная информация, включенная в Перечень сведений, составляющих коммерческую тайну предприятия, доступ к которой ограничивается в соответствии с законодательством РК;

— нарушение информационной безопасности – факт несанкционированного или непреднамеренного действия (операции) над информационной сферой, приводящий к нежелательным для предприятия последствиям;

— несанкционированный доступ – нарушение регламентированного доступа к объекту защиты;

— обработка информации – совокупность операций сбора, накопления, ввода, вывода, приёма, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения, осуществляемых над информацией;

— объект информатизации - совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для конфиденциальных переговоров;

— система защиты информации – совокупность органов и/или исполнителей, используемой ими техники защиты информации, а также объектов защиты, организованная и функционирующая по правилам, установленным соответствующими правовыми, организационно- распорядительными и нормативными документами в области защиты информации;

— средства связи – технические средства, используемые для формирования, обработки, передачи или приёма сообщений электросвязи либо почтовых отправлений;

— техническая защита информации – защита (не криптографическими методами) информации, содержащей сведения, составляющие государственную или коммерческую тайну, от её утечки по техническим каналам, от несанкционированного доступа к ней, от специальных воздействий на информацию в целях её уничтожения, искажения и блокирования, и противодействие техническим средствам разведки;

— угроза безопасности информации - совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированным и/или непреднамеренным воздействиям на неё;

— утечка информации - неконтролируемое распространение защищаемой информации в результате её разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками;

— шифрование – способ защиты информации, заключающийся в криптографическом преобразовании информации по специальному алгоритму для получения шифротекста и позволяющий предотвратить ее несанкционированное использование;

— цифровая подпись – дополнительные данные или криптографическое преобразование какого-либо блока данных, позволяющие получателю блока данных убедиться в

подлинности отправителя и целостности блока данных и защитить его от искажения с помощью, например, средств получателя.

Формы нарушения информационной безопасности:

а) пассивные

- получение информации нарушителем для использования в своих целях;
- анализ характеристик информации без доступа к самой информации;

б) активные

- изменение информации;
- внесение ложной информации
- нарушение (разрушение) информации;
- нарушение работоспособности системы обработки информации.
-

Принципы информационной безопасности:

- системный подход, предусматривающий комплексное решение проблемы информационной безопасности;
- ответственность всех сотрудников ТОО ;
- непрерывность мер информационной безопасности;
- документальность любого действия в информационной системе для установления в последующем причины, авторства и самого факта совершения действия;
- компетентность в осуществлении мер информационной безопасности.

2. Система информационной безопасности

2.1. Состав системы

Общее руководство системой информационной безопасности и принятие всех решений по вопросам ее функционирования осуществляет ответственный по технике безопасности ТОО.

Исполнительные органы системы:

- Управление по защите информации ответственный по технике безопасности;
- структурные подразделения ТОО;

Организационные средства:

- настоящая Инструкция;
- отдельные руководящие документы на время их действия;
- указания руководства ТОО;
- инструкции по эксплуатации средств информатизации в части информационной безопасности;
- протоколы информационных обследований;
- обязательства о неразглашении сведений, составляющих коммерческую тайну ТОО;
- журналы учета, установленные настоящей Инструкцией.

Технические средства:

- средства защиты от несанкционированного доступа к персональным компьютерам, программному обеспечению, сетям и информации;
- криптографические средства защиты компьютерной информации;
- средства защиты некомпьютерной информации.

2.2.1 Руководители подразделений ТОО

Руководители структурных подразделений ТОО несут персональную ответственность за организацию системы информационной безопасности в подчиненном подразделении и решают следующие задачи:

- осуществляют руководство работой по обеспечению информационной безопасности в подразделении;
- организуют проведение первичного и контрольных информационных обследований подразделения, совместно с заместителем директора утверждают Актами результаты информационных обследований;
- после согласования с заместителем директора принимают решение о предоставлении прав доступа к информации подразделения сотрудникам подчиненного подразделения и передают эти решения администратору сети для реализации;
- ходатайствуют перед руководителями других подразделений о предоставлении прав доступа к информации этих подразделений сотрудникам подчиненного подразделения;
- совместно с коммерческим департаментом и административным отделом участвуют в разработке решений по защите информации для вновь принимаемых в эксплуатацию в подразделении объектов информатизации;
- готовят и направляют в отдел заявки на установку специальных средств защиты информации, обучение сотрудников по вопросам информационной безопасности;
- взаимодействуют с отделом по вопросам организации информационной безопасности.

2.2.2. Сотрудники подразделений ТОО

Сотрудники подразделений несут ответственность за соблюдение информационной безопасности на закрепленных участках работы. Сотрудники подразделений:

- выполняют индивидуальные процедуры получения доступа к объектам информатизации и защищаемой информации;
- эксплуатируют пользовательские средства защиты информации, установленные на рабочих местах (если такие имеются);
- контролируют состояние информационной безопасности на своих рабочих местах.

2.3. Информационное обследование

Информационное обследование включает в себя первичное обследование, приводящееся однократно при создании системы информационной безопасности, и контрольные обследования, приводящиеся по мере необходимости актуализации сведений об информационной системе. Первичное информационное обследование имеет целью составление полной информационной схемы и категорирование информации, объектов информатизации, помещений и сотрудников подразделений ТОО.

Обследование состоит в полной проверке всех имеющихся рабочих мест на наличие на них информации, средств информатизации, программных продуктов и составления комплекта документов, содержащих спецификацию этих средств с точки зрения информационной безопасности и закрепляющих их текущее состояние.

Обследование проводится отдельно по подразделениям, а также в локальной вычислительной сети.

Мероприятия обследования подразделения организует руководитель подразделения, а непосредственно проводят сотрудники административного отдела, и, при необходимости, сотрудники подразделения. Результатом обследования подразделения являются документы:

1. Информационная схема подразделения (исполняется руководителем подразделения) в составе:
   - инвентарный план размещения средств информатизации и средств защиты информации подразделения с указанием их технических характеристик;
   - перечень программных продуктов, установленных на каждом из средств информатизации или доступных с этого средства в сети и информации, обрабатываемой этими программными продуктами;
   - список сотрудников подразделения с указанием закрепленных за ними средств информатизации и выделенных для них прав доступа;

2. Протоколы категорирования:
   - информации;
   - средств информатизации;
   - помещений подразделения;
   - сотрудников управления;

3. Протокол выявленных недостатков по обеспечению информационной безопасности с рекомендациями по ее совершенствованию;

4. Частный Акт информационного обследования подразделения, закрепляющий текущее состояние информационной системы, описанное в Информационной схеме, подписываемый администратором сети и сотрудником отдела и утверждаемый начальником отдела;

5. План устранения недостатков и реализации рекомендаций информационного обследования.

Мероприятия обследования локальной вычислительной сети организует начальник отдела, а непосредственно проводит. Результатом обследования сети являются документы:

1. Информационная схема локальной вычислительной сети (исполняется администратором сети) в составе:
   - топологическая схема сети с указанием трасс прокладки кабелей, мест размещения серверов, сетевого оборудования и рабочих станций, привязанная к поэтажному плану здания;
   - перечень программных продуктов, установленных в сети и информации, обрабатываемой этими программными продуктами;
   - список пользователей сети с указанием, выделенных им прав доступа;

2. Протокол категорирования программных продуктов и информации сети;

3. Протокол выявленных недостатков по обеспечению информационной безопасности с рекомендациями по ее совершенствованию;

4. Частный Акт информационного обследования локальной вычислительной сети, закрепляющий текущее состояние информационной системы, описанное в Информационной схеме, подписываемый администратором сети (специалистом) и утверждаемый начальником отдела

5. План устранения недостатков и реализации рекомендаций информационного обследования.

Контрольные информационные обследования проводятся по планам административного департамента и вне планов – в случаях:

- реорганизации подразделений;
- крупных изменений в системе делопроизводства, составе оборудования и программного обеспечения;
- перемещений подразделений в другие помещения.

2.4. Категорирование

Категорирование – это специальная классификация различных объектов, имеющих отношение к информационной системе ТОО, по признаку конфиденциальности используемой информации и, соответственно, требуемого уровня ее защиты. В ходе категорирования все объекты разбиваются на группы (категории), для каждой из которых разрабатывается собственный уникальный комплекс мер защиты.

Категорированию подвергаются:

- используемая информация;
- средства;
- помещения;
- сотрудники подразделений.

Категорирование производится в ходе первичного информационного обследования и уточняется при контрольных обследованиях. Настоящей Инструкцией вводятся следующие категории объектов информационной системы:

2.5. Документирование

Основной формой документа в системе информационной безопасности является двусторонний Акт, который составляется и подписывается сотрудниками подразделения, в котором проводится мероприятие, с одной стороны, и сотрудниками отдела с другой стороны. Акт утверждается начальником этого подразделения и начальником отдела. К Акту прилагаются необходимые в каждом конкретном случае документы: протоколы, справки, схемы и т.д., исполненные в произвольной форме.

По решению заместительного директора Акты могут докладываться для ознакомления и принятия решения.

В обязательном порядке составляются Акты в следующих случаях:

- при проведении первичного и контрольных информационных обследований;
- при проведении проверок состояния информационной безопасности Управлением по защите информации;
- при предоставлении или изменении прав доступа к информации, средствам информатизации и сотрудникам;
- при выявлении нарушений информационной безопасности и их устранении.

2.6. Обучение персонала

Сотрудники ТОО (сотрудники отдела), непосредственно принимающие участие в обеспечении информационной безопасности, могут направляться на специальное обучение. Остальные сотрудники ТОО проходят инструктаж.

3. Обеспечение информационной безопасности

3.1. Общие положения

Обеспечение информационной безопасности включает комплекс повседневно проводимых мероприятий, а именно:

- допуск (предоставление прав доступа) к информации, средствам информатизации и в помещения;
- доступ к информации, средствам информатизации и в помещения в соответствии с предоставленными правами;
- содержание средств информатизации;
- обеспечение безопасности информации;
- использование средств защиты информации;
- контроль состояния информационной безопасности;
- действия в случае выявления нарушений информационной безопасности;
- инструктаж по информационной безопасности.

3.2. Допуск

Допуск – это комплекс мероприятий, проводимых с целью предоставления прав доступа сотрудникам ТОО, представителям сторонних организаций и посетителям в помещения, к средствам информатизации и к информации ТОО.

Допуск заключается в предоставлении соответствующих прав доступа и документальном закреплении их за конкретным лицом, которому они предоставляются.

Право предоставления допуска имеет только руководитель подразделения, в ведении которого находятся объекты, к которым допускается указанное лицо, после обязательного согласования– заместительным директором. Руководитель подразделения полностью отвечает за соответствие

уровня допуска задачам, решаемым допускаемым лицом. При этом должен строго соблюдаться принцип предоставления сотрудникам минимальных прав, достаточных для выполнения задач.

Допуск может предоставляться:

- сотрудникам своего подразделения;
- сотрудникам других подразделений;
- сотрудникам сторонних организаций, выполняющим работы по заказу ТОО с заключением контракта;
- сотрудникам государственных органов, имеющим соответствующие полномочия;
- посетителям.

Различаются постоянный и разовый допуск. Постоянный допуск предоставляется только сотрудникам ТОО или представителям сторонних организаций, выполняющим работы по контракту. Разовый допуск предоставляется как сотрудникам ТОО, так и иным лицам, в том числе посетителям.

Порядок действий по предоставлению допуска зависит от того, к какому объекту допускается лицо, какова категория этого объекта, постоянный это допуск или разовый и кому он предоставляется: сотруднику своего подразделения, сотруднику другого подразделения, представителю сторонней организации или посетителю.

Допуск оформляется в письменной форме – для объектов категорий И-0, И-1, С-0, С-1, П-0, П-3 лицам, занимающим должности категорий Д-1…Д-3. Должностные лица категории Д-0 имеют допуск ко всей информации ТОО по положению. Лица категорий Д-5…Д-7 получают ограниченный допуск к отдельным массивам информации.

Допуск к объектам категорий И-2, С-2, П-4 обеспечивается устными распоряжениями руководителей подразделений.

Допуск к объектам категории П-1 предоставляется лицам всех категорий секретарями по указанию соответствующих руководителей.

Допуск к объектам категории П-2 может быть только разовым и осуществляется лицами, ответственными за организацию заседаний, совещаний и других мероприятий.

Постоянный допуск во всех случаях оформляется Актом, который составляется в подразделении в 2-х экземплярах, подписывается его сотрудниками, согласовывается с Членом Правления - Директором по безопасности и защите информации и утверждается руководителем подразделения. Допускается составление одного общего Акта сразу на нескольких сотрудников. В Акте для каждого сотрудника указываются подразделение, должность, фамилия, имя, отчество, перечень объектов, к которым предоставляется доступ, с указанием категории каждого объекта, цели доступа и предоставляемых прав, календарный период, на который предоставляется допуск. Первый экземпляр Акта хранится в департаменте, второй экземпляр Акта хранится в подразделении.

Сотрудникам других подразделений руководитель подразделения предоставляет постоянный допуск к подведомственным объектам на основании служебных записок от руководителей соответствующих подразделений, согласованных с заместительным директором.

Максимальный срок постоянного допуска – 1 год, после чего он должен переоформляться.

Постоянный допуск сотрудникам сторонних организаций, выполняющим работы по контракту, предоставляется руководителем подразделения, ответственного за сопровождение контракта, после согласования с заместительным директором при условии, что в контракте предусмотрены обязательства партнера по выполнению требований информационной безопасности и сохранению коммерческой тайны.

Разовый допуск предоставляется руководителем подразделения после согласования с управляющим директором и оформляется письменно:

- сотрудникам своего подразделения – соответствующей записью в Журнале учета доступа за подписью руководителя подразделения;
- сотрудникам других подразделений – на основании служебной записки на имя начальника допускающего подразделения, соответствующей записью в Журнале учета доступа за подписью руководителя подразделения;
- сотрудникам сторонних организаций, выполняющих работы по контракту, - на основании служебной записки от подразделения, ответственного за проведение работ, на имя начальника допускающего подразделения, соответствующей записью в Журнале учета доступа за подписью руководителя подразделения;
- посетителям – соответствующей записью в Журнале учета доступа за подписью руководителя подразделения.

Не может быть предоставлен допуск:

- постоянный и разовый – сотрудникам сторонних организаций и посетителям к информации категории И-0 (посетителям – также и к информации категории И-1);
- постоянный и разовый – сотрудникам сторонних организаций и посетителям к средствам категорий С-0, С-1, если технически не исключена возможность их несанкционированного использования;
- постоянный – сотрудникам сторонних организаций в помещения категорий П-0, П-1, и П-2;
- постоянный и разовый – посетителям в помещения категорий П-0 и П-3;
- постоянный – посетителям в помещения категорий П-1, П-2.

Представителям государственных органов может быть предоставлен допуск к любым объектам информационной системы, но только разовый и в строгом соответствии с имеющимися у них полномочиями. Необходимость допуска письменно в обязательном порядке согласовывается с заместительным директором.

Сотрудникам охраны (дежурных смен) предоставляется допуск во все помещения, категорированные по информационной безопасности, для выполнения ими обязанностей по обеспечению физической безопасности объектов.

3.3. Доступ

Доступ – это совокупность действий, выполняемых сотрудниками подразделений:

- с целью получения возможности использования информации в соответствии с имеющимся у них допуском;
- с целью предоставления возможности использования информации сотрудниками других подразделений, сторонних организаций, государственных органов и посетителями.

Таким образом, действия по доступу выполняются только сотрудниками допускающего подразделения, даже если допускаются иные лица.

Порядок доступа в помещения категории П-0…П-2 определяется руководством ТОО индивидуально. Учет доступа в помещения категории П- 3 ведут сотрудники охраны (ЧОП). Доступ в помещения категории П-4 не учитывается. Учет доступа к средствам информатизации и информации в локальной вычислительной сети ведет.

Для учета доступа в отделе информационных технологий и в охране (ЧОП) заводятся Журналы учета доступа, в которых регистрируются факты получения доступа в зависимости от вида объекта информационной системы и его категории. Учету в Журнале доступа подлежат все факты предоставления доступа всем лицам, имеющим разовый допуск к информационным объектам категорий П-0, С-0, С-1, И-0, И-1.

Общая задача доступа подразделяется на подзадачи:

- доступ в помещения;
- доступ к средствам информатизации;
- доступ к программным продуктам и информации.

Действия по осуществлению доступа подразделяются на организационные и технические. Ответственность за организацию доступа несет руководитель подразделения, а за правильное выполнение действий по доступу – сотрудник, их выполняющий.

3.3.1. Доступ в помещения

Доступ в помещения сотрудников, чьи рабочие места находятся в этих помещениях, осуществляется в соответствии с Инструкцией о пропускном режиме охраны (ЧОП) с учетом присвоенных этим помещениям категорий информационной безопасности.

Доступ в помещения сотрудников своего подразделения и сотрудников других подразделений, чьи рабочие места расположены в других помещениях, зависит от категории помещения:

- в помещения категории П-0 доступ возможен только при наличии соответствующего допуска через того из сотрудников, работающих в помещении, к которому этот посетитель прибыл;
- в помещения категории П-3 и П-4 доступ свободный.

Доступ в помещения сотрудников сторонних организаций и представителей государственных органов возможен только при наличии соответствующего допуска через того из сотрудников, работающих в помещении, к которому этот посетитель прибыл.

Доступ в помещения категории П-1 контролируется в рабочее время секретарями, в нерабочее время – сотрудниками охраны. Нахождение в этих помещениях кого бы то ни было, кроме владельцев кабинетов, секретарей и сотрудников охраны, без сопровождения секретарей (в рабочее время) или сотрудников охраны (в нерабочее время) строго запрещается.

Технические действия по доступу в помещения зависят от того, оборудованы ли помещения соответствующими техническими средствами и, как правило, состоят в снятии помещения с контроля системой охранной сигнализации и вскрытие помещения установленным порядком в начале рабочего дня.

Организационные действия по доступу в помещения выполняются сотрудниками, работающими в них, и заключаются в:

- проверке состояния помещения и находящихся в нем средств информатизации при вскрытии помещения и перед его закрытием;
- принятии мер по недопущению в помещения посторонних лиц, не имеющих допуска или нарушающих правила доступа;
- учете доступа в помещения в Журнале учета доступа там, где это необходимо.

Порядок доступа в помещения сотрудников охраны:

- в помещения категории П-0…П-3 – только в случаях прямой необходимости, в рабочее время - вместе с сотрудником, работающим в данном помещении, в нерабочее время - с последующим составлением служебной записки на имя директора ЧОП за подписью начальника смены с изложением причин доступа и описанием состояния помещения;
- в помещения категории П-4 – без ограничений.

3.3.2. Доступ к средствам информатизации

Доступ к средствам информатизации, находящимся на рабочих местах сотрудников(далее – «ответственные за средства информатизации»), осуществляется этими сотрудниками без ограничений.

Доступ к средствам информатизации сотрудников других подразделений, представителей сторонних организаций, представителей государственных органов и посетителей осуществляется в зависимости от категории:

- к средствам информатизации категорий С-0, С-1 – только при наличии допуска. При этом непосредственное использование средства информатизации осуществляется сотрудником, ответственным за него, а лицо, получившее доступ, присутствует при этом;
- к средствам информатизации категории С-2 – самостоятельно и без ограничений.

Для средств информатизации категорий С-0 и С-1 в отделе информационных технологий должен быть заведен Аппаратный журнал, в котором отражаются все критичные операции и события (выход из строя, ремонт, техобслуживание и т.п.), а также операции по обеспечению информационной безопасности.

Управлению информационных систем и технологий категорически запрещёно подключение средств информатизации категорий С-0 и С-1 к ресурсам и сервисам международной компьютерной сети Internet. Локальная вычислительная сеть, имеющая в своём составе средства информатизации категорий С-0 и С-1 не может иметь выход в международную сеть Internet.

Технические действия по осуществлению доступа заключаются в:

- включении питания;
- преодолении установленным порядком имеющихся средств защиты доступа (замок, вход по паролю, идентификация пользователя и др.).

Организационные действия заключаются в:

- ведении Аппаратного журнала;

— ведении Журнала учета доступа.

После того, как операции по доступу к средствам категорий С-0, С-1 выполнены, ответственный за средство информатизации обязан обеспечить невозможность использования средства кем-либо, кроме него самого. Запрещается даже на короткое время оставлять без контроля средство информатизации, если такая возможность не исключена технически.

Для доступа к средствам информатизации там, где это возможно, в обязательном порядке должен использоваться пароль, а доступ должен быть организован строго в соответствии с Руководством по применению паролей.

3.3.3. Доступ к программным продуктам и информации

Порядок получения доступа к программным продуктам и информации определяется порядком доступа в помещения и к средствам информатизации. Ответственность за правильность доступа к программным продуктам и информации несут сотрудники, на рабочих местах которых используются эти программные средства и информация.

Доступ обеспечивается:

— к программным продуктам и компьютерной информации – имеющимися программно-аппаратными средствами защиты;
— к информации на бумажных носителях – принятой технологией несекретного «бумажного» делопроизводства;
— к речевой, видео- и другим видам информации – мерами обеспечения доступа в помещения и к средствам связи.

Технические действия по доступу к программным продуктам и информации заключаются в:

— запуске программного продукта;
— преодолении установленным порядком имеющихся программных и аппаратных средств защиты;
— регистрации доступа средствами регистрации, если они имеются.

Организационные действия по доступу к программным продуктам и информации заключаются в ведении Журнала учета доступа.

3.4. Содержание средств информатизации

Правильное с точки зрения информационной безопасности содержание (эксплуатация и хранение) средств информатизации предполагает:

— для средств информатизации категории С-0 – полное предотвращение доступа (в том числе и физического) к этим средствам любых лиц, не имеющих соответствующего допуска;
— для средств информатизации категории С-1 – предотвращение несанкционированного их использования;
— для средств информатизации категории С-2 – ограничений нет.

Содержание программных продуктов средств информатизации определяется содержанием технических средств информатизации (компьютеров, сетей), на которых эти программные продукты установлены.

Средства информатизации содержатся, как правило, на рабочих местах сотрудников, за которыми эти средства закреплены. Технические средства категории С-0 могут содержаться в кладовых или в сейфах.

В рабочее время ответственность за содержание средств информатизации несут сотрудники, за которыми эти средства закреплены, а в их отсутствие – их непосредственные начальники. В нерабочее время ответственность за хранение средств информатизации несет дежурная смена охраны.

Приемка в эксплуатацию средств информатизации (аппаратных, программных) категорий С-0 и С-1 проводится силами сотрудников отдела в следующем порядке:

- определяется категория средства информатизации;
- средство информатизации оснащается программными продуктами, устанавливается на рабочем месте и проверяется;
- производится проверка безопасности средства информатизации; при необходимости для такой проверки могут привлекаться специализированные организации;
- составляется и согласовывается с соответствующим подразделением перечень организационно-технических мероприятий, необходимых для обеспечения информационной безопасности средства информатизации, в том числе перечень средств защиты информации;
- средство информатизации, при необходимости, дополняется средствами защиты информации, из него исключаются не используемые «опасные» устройства и опечатывается;
- средство проверяется сотрудниками подразделения на предмет готовности к эксплуатации;
- составляется Акт о готовности средства информатизации по вопросам информационной безопасности, который утверждается заместительным директором принимающего подразделения.

Каждое средство информатизации после приемки в эксплуатацию закрепляется письменным распоряжением руководителя подразделения за одним из сотрудников подразделения, который в дальнейшем отвечает за его содержание.

Сотрудник, ответственный за содержание средства информатизации, в части обеспечения информационной безопасности обязан:

- обеспечить установленный порядок доступа к средству информатизации;
- правильно использовать средства защиты информации, с которыми работает средство информатизации, если они имеются;
- при обнаружении признаков несанкционированного доступа к средству информатизации немедленно прекратить все работы с ним, обеспечить сохранение его в текущем состоянии и сообщить о случившемся своему руководителю и Начальником отдела.

Учет средств информатизации ведется отделом информационных технологий в Журнале учета средств информатизации:

- технические средства информатизации учитываются в соответствии с их инвентарными номерами, которые присваиваются им при приемке в эксплуатацию;
- программные продукты средств информатизации учитываются по экземплярно.

Дистрибутивы программных продуктов хранятся администратором сети таким образом, чтобы исключить возможность использования их для инсталляции несанкционированных копий программного продукта. Инсталляцию прикладных и автономных программных продуктов выполняет.

Рабочие копии программных продуктов должны быть защищены от несанкционированной модификации программного кода и данных, для чего должны применяться различные методы, в том числе:

- установка программных продуктов на средствах информатизации соответствующей категории;
- установка программных продуктов на серверах сети с разделением доступа к ним, исходя из категорий пользователей;
- защита программных продуктов от копирования;
- шифрование исполняемых модулей и данных программных продуктов на носителях информации;
- запуск особо охраняемых программных продуктов категории С-0 и работа с информацией категории И-0 с гибких магнитных дисков, хранимых в сейфах.

Если доступ к средству информатизации защищается устройствами типа «замок» (механические замки, электронные замки, кодовые устройства и т.п.), имеющими «ключи» (обычные ключи, магнитные карты и т.п.), то оригинал ключа хранится у ответственного сотрудника, а дубликаты – у руководителя соответствующего подразделения. Хранение оригинала и дубликатов должно быть обеспечено таким образом, чтобы исключить возможность попадания ключа к кому-либо, кроме этих лиц. Все экземпляры ключей учитываются отдельными позициями в Журнале учета средств информатизации. В случае утраты ключа принимаются такие же меры, как при выявлении попытки несанкционированного доступа.

3.5. Обеспечение безопасности информации

Безопасность информации обеспечивается в соответствии с присвоенными ей категориями и предполагает:

- для информации категории И-0 – полное исключение возможности несанкционированного доступа к ней;
- для информации категории И-1 – исключение возможности несанкционированной модификации, предупреждение возможности анализа и статистической оценки;
- для информации категории И-2 – ограничений нет.

Основой безопасности информации является изложенная в п. 3.3. система контролируемого доступа в помещения, к средствам информатизации и самой информации. Кроме этого, в зависимости от формы представления информации, с целью обеспечения ее безопасности принимаются специальные меры, изложенные ниже. Во всех случаях, за исключением специально оговоренных, ответственность за принятие этих мер несет сотрудник, использующий информацию или организующий мероприятие с ее использованием.

Безопасность информации в бумажной форме представления обеспечивается в соответствии с принятой технологией «бумажного» документооборота.

Для обеспечения безопасности речевой информации необходимо:

- ограничить число лиц, участвующих в переговорах, до минимально необходимого;
- проводить переговоры в местах, исключающих возможность подслушивания;
- применять специальные средства, если такие имеются.

Для обеспечения безопасности телефонных переговоров необходимо:

- безусловно исключить из обсуждения при ведении переговоров по открытым (незащищенным) телефонным линиям связи сведения, относящиеся к категории И-0 и ограничивать использование сведений категории И-1;
- применять специальные средства, если такие имеются.

Для обеспечения безопасности информации, обрабатываемой с помощью средств информатизации необходимо:

- обеспечить защиту от несанкционированного получения информации категории И-0 и защиту от модификации, а также возможность восстановления авторства доступа к информации категорий И-0, И-1, для чего в обязательном порядке применять все меры защиты, доступные на используемых программно-аппаратных средствах;
- обеспечить хранение носителей информации (дискет, магнито- оптических дисков, компакт-дисков и др.) с информацией категории И-0 способом, исключающим их утрату, несанкционированное копирование и получение;
- обеспечить хранение применяемых средств защиты информации, в том числе средств доступа к ним, способом, исключающим их несанкционированное использование.

3.6. Использование средств защиты информации

Средства защиты информации – это специальные технические средства, используемые для предупреждения несанкционированного использования всех видов информации. Разнообразие видов используемой информации, целей защиты, вариантов угроз, применяемых технологий защиты определяют широкую номенклатуру таких средств. В каждом случае необходимости защиты информации выбирается свой конкретный тип средства.

По вариантам использования различаются средства защиты информации:

- коллективные, применяемые для защиты информации, используемой одновременно несколькими (многими) сотрудниками;
- индивидуальные, применяемые только одним сотрудником для защиты информации, используемой им самим;
- сетевые, применяемые для защиты в вычислительных сетях и сетях связи.

Необходимость применения средств защиты информации определяется при информационном обследовании, при принятии решения о применении

информационной техники и в других случаях. Принятие решения на применение средств защиты, выбор способа защиты и типа средства защиты информации осуществляется совместно подразделением, которое использует защищаемую информацию, управляющим директором и утверждается Президентом.

Решение о применении средств защиты информации в подразделении оформляется совместным документом этого подразделения и, утверждается управляющим директором и представляется руководителем подразделения, защищающего свою информацию, для утверждения и выделения необходимых финансовых и технических средств Президенту ТОО.

Закупку средств защиты информации производит отдел бухгалтерского учета и экономического планирования. Если поставляемые средства защиты входят в состав средств информатизации (систем), их закупку (заказ разработки) выполняет подразделение, закупающее (заказывающее разработку) по согласованию с коммерческим департаментом.

Ответственность за использование средств защиты информации несут:

- за средства защиты коллективного пользования – специально назначаемые сотрудники;
- за средства защиты индивидуального пользования – сотрудники, на рабочих местах которых эти средства установлены;
- за сетевые средства защиты

Закрепление средств защиты информации за ответственными за них сотрудниками производится письменным распоряжением руководителя соответствующего подразделения, первый экземпляр которого представляется и хранится в административном департаменте.

Порядок приемки в эксплуатацию средств защиты информации:

- средство устанавливается администратором сети на рабочем месте и проверяется в соответствии с инструкцией по эксплуатации;
- сотрудник и отдела составляют и подписывают совместный Акт о приемке с приложением необходимых материалов и утверждают его у руководителя принимающего подразделения и начальника отдела, после чего средство считается принятым в эксплуатацию;
- средство защиты информации передается в эксплуатацию назначенному ответственному сотруднику.

Сотрудник, ответственный за средство защиты информации, обязан:

- изучить средство в объеме, необходимом для правильной его эксплуатации;
- обеспечить установленный порядок использования средства: своевременно включать и выключать его, поддерживать эффективный режим работы;
- не допускать несанкционированного применения средства кем бы то ни было, обеспечить его сохранность, сообщать в административный департамент обо всех попытках несанкционированного использования средства или подозрениях на такие попытки;
- проводить техническое обслуживание, обеспечивать его исправность, организовывать ремонт в случае выхода из строя и выполнять другие эксплуатационные операции.

Учет средств защиты информации ведется отделом ИТ в отдельном разделе Журнала учета средств информатизации в соответствии с их инвентарными номерами, которые присваиваются им при приемке в эксплуатацию.

3.7. Контроль состояния информационной безопасности

Контроль состояния информационной безопасности проводится с целью проверки ее организации, а также предупреждения и своевременного выявления случаев ее нарушения.

Обязанности по контролю распределяются между заместительными органами системы информационной безопасности следующим образом:

- отдел проводит проверки организации и состояния информационной безопасности в подразделениях;
- сотрудники контролируют текущее состояние информационной безопасности на своих рабочих местах;
- повседневно контролирует текущее состояние информационной безопасности в локальной вычислительной сети;
- руководители подразделений повседневно контролируют текущее состояние информационной безопасности в своих подразделениях;
- сотрудники контролируют текущее состояние информационной безопасности на своих рабочих местах.

Проверки организации и состояния информационной безопасности проводятся административным департаментом в подразделениях и в сетях и могут быть:

- плановыми;
- внезапными;
- по фактам нарушения информационной безопасности.

Плановые проверки проводятся в соответствии с годовым Планом проверок, который составляется на очередной год в декабре текущего года, подписывается и утверждается Директором ТОО. В ходе плановых проверок должна полностью проверяться вся организация системы информационной безопасности.

Внезапные проверки проводятся административном департаменте соответствии с внутренними планами работы. Внезапные проверки проводятся по отдельным вопросам организации информационной безопасности.

Проверки по фактам нарушения информационной безопасности проводятся административным департаментом после того, как нарушение устранено. Проверка проводится с целью выявления причин и предпосылок нарушения и выработки мер по предупреждению подобных нарушений в дальнейшем. Проверка проводится в обязательном порядке по каждому факту нарушения независимо от его последствий.

Результаты всех проверок оформляются двусторонними Актами между проверяющей и проверяемой сторонами, с необходимыми в каждом конкретном случае приложениями и утверждаются заместительным директором. При возникновении разногласий с проверяемым подразделением может оформляться односторонний Акт отдела.

Для текущего контроля состояния информационной безопасности независимо от работы информационной системы и сотрудников ТОО отдела должны применяться специальные средства, такие как специальное автоматизированное рабочее место (АРМ безопасности),

различные технические средства для оценки эффективности применяемых методов и средств обеспечения безопасности.

Контролирует состояние информационной безопасности на подведомственных участках:

- контролирует выполнение сотрудниками установленного порядка действий по доступу к объектам информационной системы;
- анализирует состояние информационной системы с целью выявления попыток несанкционированного доступа и использования средств информатизации и информации;
- контролирует правильность использования имеющихся коллективных и индивидуальных средств информационной защиты.

В случае выявления каких-либо отклонений или нарушений в системе информационной безопасности немедленно обязан принять все меры к их устранению самостоятельно, через руководителя соответствующего подразделения или с привлечением административным департаментом. Ответственность за принятие этих мер и сообщение о происшедшем руководителю подразделения и в административно- правовой отдел несет.

Сотрудники подразделений анализируют состояние своих рабочих мест с целью выявления попыток несанкционированного доступа и использования средств информатизации и информации. В случае выявления таких попыток сотрудник немедленно обязан сообщить об этом администратору сети и своему руководителю.

3.8. Порядок действий в случае выявления нарушений информационной безопасности

Действия, предпринимаемые в случае выявления нарушений информационной безопасности, состоят в следующем:

- выявление факта нарушения;
- прекращение всех операций, связанных с участком, на котором произошло нарушение;
- принятие экстренных мер для прекращения несанкционированного доступа или использования информации;
- оповещение о нарушении;
- восстановление работоспособности информационной системы;
- расследование причин нарушения информационной безопасности;
- проверка состояния информационной безопасности по факту нарушения.

Выявление факта нарушения, как правило, происходит в ходе контроля состояния информационной безопасности сотрудником подразделения, администратором сети или сотрудниками отдела.

Немедленно после выявления нарушения сотрудник, который обнаружил его, обязан прекратить все операции по использованию по назначению информации и средств информатизации, которые выполнялись на участке, где произошло нарушение, а также, если необходимо, на смежных участках. Если выявлен несанкционированный доступ в категорированные помещения, всякий доступ в него должен быть прекращен.

Если на момент выявления нарушения несанкционированный доступ или использование средств информатизации и информации еще продолжаются, сотрудник, выявивший их, обязан немедленно принять меры к их прекращению. Конкретное содержание этих мер зависит от того,

каков характер нарушения, то есть информационный объект какой категории попал под нарушение, какой ущерб может быть нанесен нарушением, какие побочные последствия повлечет принятие этих мер. По возможности следует привлечь для выработки и принятия мер администратора сети, руководителя подразделения, сотрудников отдела. Ответственность за адекватность принимаемых мер несут в порядке привлечения сотрудник, выявивший нарушение, и руководитель подразделения.

После того, как нарушение выявлено и блокировано, производится срочное оповещение о нем в следующем порядке:

- сотрудник оповещает руководителя своего подразделения, административный департамент;
- руководитель подразделения оповещает других сотрудников своего подразделения на участках ответственности которых могут возникнуть подобные нарушения;

С целью минимизации ущерба от прекращения работы информационной системы немедленно после того, как возможность дальнейшего нарушения информационной безопасности устранена, принимаются меры для восстановления ее работы. Решение на восстановление работы принимает руководитель подразделения, на участке ответственности которого произошло нарушение, по согласованию с административным департаментом.

Расследование причин нарушения производится административным департаментом, при этом все связанные с нарушением сотрудники должны оказывать содействие расследованию. Целью расследования является выявление истинных причин нарушения и предпосылок к нему для принятия мер к недопущению его повторения. Расследование проводится сразу после восстановления работоспособности информационной системы, в обязательном порядке, независимо от последствий, которые повлекло нарушение. Результаты расследования оформляются двусторонним Актом Административным отделом, подразделения, в котором произошло нарушение и утверждаются заместительным директором.

По факту нарушения в отделе проводится также проверка системы информационной безопасности на тех ее участках, где подобные нарушения возможны.

Доклад о факте нарушения и ходе работ по его устранению руководству ТОО производится в зависимости от характера нарушения и размера возможного ущерба от него. Ответственность за своевременность доклада несет руководитель подразделения, в котором произошло нарушение (первая очередь) и руководство административного отдела.

3.9. Инструктаж

Для обучения сотрудников и иных лиц, имеющих допуск к информации ТОО , правилам обеспечения информационной безопасности и поддержания их знаний и навыков в соответствии с текущей обстановкой на рабочих местах организуется их инструктаж. Проводятся следующие виды инструктажа:

- вводный;
- периодический;
- разовый.

Инструктаж проводит сотрудник административного департамента.

Кроме этих видов инструктажа, при допуске сотрудника и иных лиц в качестве пользователя сети проводит с ним вводный инструктаж.

При вводном инструктаже сообщаются сведения:

- категория должности, занимаемой сотрудником;
- перечень средств информатизации и программных продуктов, имеющихся на его рабочем месте и смежных рабочих местах, их категории;
- перечень помещений, в которые он имеет допуск, их категории;
- перечень информации, к которой он имеет допуск, и его права доступа к ней;
- порядок доступа и работы с каждым из названных объектов в соответствии с его категорией, при необходимости содержание Руководства по применению паролей;
- порядок содержания средств информатизации;
- порядок обеспечения безопасности информации;
- порядок использования средств защиты информации, если они имеются;
- обязанности сотрудника по контролю за информационной безопасностью;
- возможные варианты нарушений информационной безопасности на конкретном рабочем месте;
- действия при выявлении нарушений информационной безопасности.

Периодический инструктаж проводится один раз в год. В периодический инструктаж включается краткое изложение вопросов вводного инструктажа и подробное – изменений по этим вопросам, произошедшим со времени предыдущего инструктажа.

Разовый инструктаж проводится при проведении отдельных мероприятий по обеспечению информационной безопасности.

Инструктаж пользователя сети, проводимый администратором сети, включает:

- перечень программных продуктов, сетевых устройств, разделов памяти сетевых устройств и информации, к которым пользователь имеет доступ в сети, права доступа пользователя и категории этих объектов информационной системы;
- порядок доступа в сеть, в том числе содержание Руководства по применению паролей;
- порядок использования средств защиты информации в сети, если они имеются;
- особенности контроля за информационной безопасностью, варианты ее нарушений, действия при выявлении нарушений, если эти действия носят какие-либо особенности относительно общепринятых.

Инструктаж во всех случаях оформляется соответствующей записью в Журнале инструктажа по информационной безопасности, который заводится для этих целей в отделе, и заверяется подписью инструктируемого сотрудника и лица, проводившего инструктаж.

УТВЕРЖДАЮ

Директор ТОО «Automation Technology and Solutions»

Нуртазин Е.Х.

«11» октября 2017 г.