PROFI CREDIT
Profireal Group

ООО «МКК «ПРОФИРЕАЛ»
196084, Россия, Санкт-Петербург
Лиговский пр., дом 266, литера «О».
Тел.: +7 (812) 424 46 44
E-mail: info@profi-credit.ru, www.profi-credit.ru

Номер:	***P8-7***
Название	***ИТ Безопасность***

ВВЕДЕНИЕ

Целью данной процедуры является обеспечение ИТ безопасности ООО «МКК «ПРОФИРЕАЛ» (далее по тексту – «Компания»), путем достижения доступности, целостности и конфиденциальности всей информации в Компании.

Процедура ИТ безопасности является локальным нормативным актом Компании.

ОТВЕТСТВЕННОСТЬ

Сотрудники Компании несут полную персональную ответственность за соблюдение требований данной процедуры и обязаны сообщать обо всех выявленных нарушениях в области информационной безопасности Специалисту по информационной безопасности, Директору отдела ИТ или лицу, его замещающему.

ТЕРМИНЫ И СОКРАЩЕНИЯ

Компания	ООО «МКК «ПРОФИРЕАЛ»
ИС	Информационные системы (CRM, NAV)
ИР	Информационные ресурсы
БД	База Данных
ЛВС	Локальная Вычислительная Сеть
АРМ	Автоматизированное Рабочее Место
НСД	Несанкционированный Доступ
ИТ	Информационные технологии
VPN	Виртуальная локальная сеть
СКУД	Системы контроля и управления доступом
S-Terra VPN Client	Программа для подключения к сети Компании
eToken	Флэш карта с электронным ключом
SmartCard	Пластиковая карта для идентификации пользователя
Biometric Sensor	Сканер отпечатка пальца
DallasLock	Система защиты от НСД
ESET	Программа для защиты ПК (Антивирус, межсетевой экран)
Исполнитель	Сотрудник или организация, привлеченная по договору для выполнения работ

СОПУТСТВУЮЩИЕ ПРОЦЕДУРЫ И ДИРЕКТИВЫ

P8-5 Запрос на изменение доступа к информационным системам и ресурсам компании

S51 Порядок использования систем контроля на рабочем месте

ООО «МКК «ПРОФИРЕАЛ»
196084, Россия, Санкт-Петербург
Лиговский пр., дом 266, литера «О».
Тел.: +7 (812) 424 46 44
E-mail: info@profi-credit.ru, www.profi-credit.ru

СОДЕРЖАНИЕ:

1. ОПИСАНИЕ ПРОЦЕССОВ

- Определение целей и задач в области информационной безопасности
- Определение объектов защиты в ИС и ИР
- Доступы к информационным ресурсам и системам Компании
- Контроль изменений в информационных системах и ресурсах Компании
- Контроль за пользователями Компании
- Работа сотрудников за пределами Компании
- Работа с внешними организациями и исполнителями
- Описание типов доступа сотрудников в сети Интернет
- Передача паролей от беспроводных точек доступа в Компании

PROFI CREDIT
Profireal Group

ООО «МКК «ПРОФИРЕАЛ»
196084, Россия, Санкт-Петербург
Лиговский пр., дом 266, литера «О».
Тел.: +7 (812) 424 46 44
E-mail: info@profi-credit.ru, www.profi-credit.ru

2. ПОДРОБНОЕ ОПИСАНИЕ ПРОЦЕССА

2.1. ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основной целью, на достижение которой направлены все положения настоящей процедуры, является защита субъектов информационных отношений (интересы которых затрагиваются при создании и функционировании ИС Компании) от возможного нанесения им ощутимого материального, физического, морального или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования ИР и ИС Компании или несанкционированного доступа к циркулирующим в них данным и их незаконного использования.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств информационных систем и ресурсов:

1. Конфиденциальность - состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на неё право.
2. Целостность - избежание несанкционированной модификации информации.
3. Доступность - состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно.

2.2. ОБЪЕКТЫ ЗАЩИТЫ

Основными объектами информационной безопасности в Компании являются:

- информационные ресурсы и системы Компании, составляющие коммерческую, финансовую, иную охраняемую законом тайну, иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы и системы, в том числе открытая (общедоступная) информация, представленнае в виде документов и массивов информации, независимо от формы и вида их представления;
- 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 чувствительные компоненты ИС.

2.2.1. Категории информационных ресурсов, подлежащих защите

В подсистемах ИС и ИР Компании циркулирует информация различных уровней конфиденциальности (секретности), содержащая сведения ограниченного распространения (служебная коммерческая, иная охраняемая законом информация, персональные данные) и открытые сведения.

ООО «МКК «ПРОФИРЕАЛ»
196084, Россия, Санкт-Петербург
Лиговский пр., дом 266, литера «О».
Тел.: +7 (812) 424 46 44
E-mail: info@profi-credit.ru, www.profi-credit.ru

В документообороте ИС и ИР Компании присутствуют:
- платежные поручения и другие расчетно-денежные документы;
- отчеты (финансовые, аналитические и др.);
- сведения о лицевых счетах;
- обобщенная информация и другие конфиденциальные (ограниченного распространения) документы.

Защите подлежит вся информация, циркулирующая в ИС и ИР Компании и содержащая, в том числе:

- сведения, составляющие коммерческую тайну, доступ к которым ограничен собственником информации в соответствии с предоставленными Федеральным законом от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации» правами;

- сведения, составляющие иную охраняемую законом тайну, доступ к которым ограничен в соответствии с законодательством Российской Федерации;
- персональные данные, доступ к которым ограничен в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных».

2.2.2. Категории пользователей информационных систем

В Компании имеется большое число категорий пользователей и обслуживающего персонала, которые должны иметь разные уровни доступа к ИС и ИР Компании:

- пользователи ИС и ИР Компании - конечные пользователи, сотрудники отделов Компании;
- ответственные за ведение баз данных (ввод, корректировка, удаление данных в БД);
- системные администраторы (файловых серверов, серверов приложений, серверов баз данных) и ЛВС;
- разработчики программного обеспечения и ответственные сотрудники за сопровождение ИС и ИР Компании на серверах и рабочих станциях пользователей;
- специалисты по обслуживанию информационных ресурсов и систем Компании.

2.2.3. Технические средства защиты

Технические (аппаратно-программные) средства защиты основаны на использовании различных электронных устройств (eToken, SmartCard, Biometric Sensor) и специальных программ (DallasLock, ESET), входящих в состав ИР и ИС Компании и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты информации (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие).

С учетом всех требований и принципов обеспечения безопасности информации в ИС и ИР по всем направлениям защиты в состав системы защиты включены следующие средства:

ООО «МКК «ПРОФИРЕАЛ»
196084, Россия, Санкт-Петербург
Лиговский пр., дом 266, литера «О».
Тел.: +7 (812) 424 46 44
E-mail: info@profi-credit.ru, www.profi-credit.ru

- средства аутентификации пользователей и элементов ИС и ИР Компании, соответствующие степени конфиденциальности информации и обрабатываемых данных;
- средства разграничения доступа к данным;
- средства криптографического закрытия информации в линиях передачи данных и в базах данных;
- средства регистрации обращения и контроля за использованием защищаемой информации;
- средства реагирования на обнаруженный НСД;
- идентификация и аутентификация пользователей при помощи имен и/или специальных аппаратных средств (eToken, Smart Card);
- регламентация доступа пользователей к физическим устройствам компьютера (дискам, портам ввода-вывода);
- избирательное (дискреционное) управление доступом к логическим дискам, каталогам и файлам;
- полномочное (мандатное) разграничение доступа к защищаемым данным на рабочей станции и на файловом сервере;
- создание замкнутой программной среды разрешенных для запуска программ, расположенных как на локальных, так и на сетевых дисках;
- защита от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ;
- контроль целостности модулей системы защиты, системных областей диска и произвольных списков файлов в автоматическом режиме и по командам администратора;
- регистрация всех действий пользователя в защищенном журнале, наличие нескольких уровней регистрации;
- централизованный сбор, хранение и обработка на файловом сервере журналов регистрации рабочих станций сети;
- защита данных системы защиты на файловом сервере от доступа всех пользователей, включая администратора сети;
- централизованное управление настройками средств разграничения доступа на рабочих станциях сети;
- оповещение системного администратора обо всех событиях НСД, происходящих на рабочих станциях;
- оперативный контроль за работой пользователей сети, изменение режимов функционирования рабочих станций и возможность блокирования (при необходимости) любой станции сети;
- поддержание в обновленном состоянии, на уровне операционной системы, информационные ресурсы, сервера и компьютеры пользователей.

Успешное применение технических средств защиты предполагает, что выполнение перечисленных ниже требований обеспечено организационными мерами и используемыми физическими средствами защиты:

ООО «МКК «ПРОФИРЕАЛ»
196084, Россия, Санкт-Петербург
Лиговский пр., дом 266, литера «О».
Тел.: +7 (812) 424 46 44
E-mail: info@profi-credit.ru, www.profi-credit.ru

- физическая целостность всех компонент ИР и ИС Компании обеспечена;
- каждый сотрудник (пользователь системы) имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ИР системы;
- использование на АРМ Компании инструментальных и технологических программ (тестовых утилит, отладчиков и т.п.), позволяющих предпринять попытки взлома или обхода средств защиты, ограничено и строго регламентировано;
- все изменения конфигурации технических и программных средств ИС и ИР производятся строго установленным порядком только на основании распоряжений Директора по ИТ;
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних лиц (специальные помещениях, шкафах, и т.п.).

2.2.4. Средства идентификации и аутентификации пользователей в ИС и ИР Компании

В целях предотвращения работы с ИС и ИР Компании посторонних лиц должна быть обеспечана возможность распознавания системой каждого законного пользователя (или ограниченных групп пользователей). Для этого в системе (в защищенном месте) хранится ряд признаков каждого пользователя, по которым этого пользователя можно опознать. В дальнейшем при входе в систему, а при необходимости - и при выполнении определенных действий в системе, пользователь себя идентифицирует, т.е. указывает идентификатор, присвоенный ему в системе в виде имени пользователя и пароля. Кроме того, для идентификации могут применяться различного рода устройства: eToken, Smart Card.

2.2.5. Доступы в помещения и к оборудованию Компании

Физическая безопасность ИР и ИС Компании обеспечена с помощью СКУД. В удаленных офисах ограничен доступ для посторонних лиц к сетевому оборудованию Компании с помощью запираемых на ключ шкафов или помещений. Назначен ответственный сотрудник в офисе, который имеет доступ к оборудованию. Запрещено производить любые работы с оборудованием Компании без согласования с ИТ отделом.

2.2.6. Средства разграничения доступа

После распознавания пользователя в системе, ему предоставляются права в ИС и ИР Компании: какие данные и как он может использовать, какие программы может выполнять, когда, как долго и с каких терминалов может работать, какие ресурсы системы может использовать и т.п. Авторизация пользователя должна осуществляется с использованием следующих механизмов реализации разграничения доступа:

ООО «МКК «ПРОФИРЕАЛ»
196084, Россия, Санкт-Петербург
Лиговский пр., дом 266, литера «О».
Тел.: +7 (812) 424 46 44
E-mail: info@profi-credit.ru, www.profi-credit.ru

- механизмов избирательного управления доступом, основанных на использовании атрибутных схем, списков разрешений и т.п.;
- механизмов полномочного управления доступом, основанных на использовании меток конфиденциальности ресурсов и уровней допуска пользователей;
- механизмов обеспечения замкнутой среды доверенного программного обеспечения (индивидуальных для каждого пользователя списков разрешенных для запуска программ), поддерживаемых механизмами идентификации (распознавания) и аутентификации (подтверждения подлинности) пользователей при их входе в систему.

2.2.7. Средства контроля и регистрации событий безопасности

Средства объективного контроля обеспечивают обнаружение и регистрацию всех событий (действий пользователей, попыток НСД), которые могут повлечь за собой нарушение политики безопасности и привести к возникновению кризисных ситуаций. Средства контроля и регистрации предоставляют возможности:

- ведения и анализа журналов регистрации событий безопасности (системных журналов). Журналы регистрации должны вестись для каждой рабочей станции сети;
- оперативного ознакомления специалиста по информационной безопасности с содержимым системного журнала любой станции и с журналом оперативных сообщений об НСД;
- оперативного оповещения системного администратора о нарушениях.

При регистрации событий безопасности в системном журнале фиксируется следующая информация:

- дата и время события;
- идентификатор субъекта (пользователя, программы), осуществляющего регистрируемое действие;
- действие (если регистрируется запрос на доступ, то отмечается объект и тип доступа).

Средства контроля должны обеспечивать обнаружение и регистрацию следующих событий:

- вход пользователя в систему;
- неудачная попытка входа в систему (неправильный ввод пароля);
- подключение к файловому серверу;
- попытка открытия файла, недоступного для чтения;
- попытка удаления файла, недоступного для модификации;
- попытка изменения атрибутов файла, недоступного для модификации;
- попытка получения доступа к недоступному каталогу;

ООО «МКК «ПРОФИРЕАЛ»
196084, Россия, Санкт-Петербург
Лиговский пр., дом 266, литера «О».
Тел.: +7 (812) 424 46 44
E-mail: info@profi-credit.ru, www.profi-credit.ru

- попытка чтения/записи информации с диска, недоступного пользователю;
- нарушение целостности программ и данных системы защиты.

Должны поддерживаться следующие основные способы реагирования на обнаруженные факты НСД:

- извещение владельца информации о НСД к его данным;
- снятие программы (задания) с дальнейшего выполнения;
- извещение специалиста по информационной безопасности;
- отключение АРМ, с которого были осуществлены попытки НСД к информации;
- исключение нарушителя из списка зарегистрированных пользователей.

По факту каждого нарушения безопасности ИТ необходимо незамедлительно уведомлять Директора по ИТ.

2.2.8. Видеонаблюдение в офисах Компании

В Компании организованно видеонаблюдение в помещениях. Данные с камер размещаются на видеорегистраторах, которые находятся в офисах, в сетевых шкафах. Срок хранения записи составляет не более 3 месяцев. К просмотру камер и записей допускается Директор по ИТ, Специалист по информационной безопасности. Дополнительный доступ к просмотру рассматривается через заявку в helpdesk от руководителя отдела. В заявке должно быть указано:

- офис, который интересует
- цель доступа
- срок предоставления доступа

После согласования доступа Специалистом по ИБ или Директором по ИТ к камерам видеонаблюдения Специалист по ИБ осуществляет настройку программного обеспечения для просмотра. Полученные логины и пароли к камерам запрещено передавать третьим лицам.

2.3. ДОСТУПЫ К ИНФОРМАЦИОННЫМ РЕСУРСАМ И СИСТЕМАМ КОМПАНИИ

Доступы и их изменения к ИС и ИР Компании определены в приложениях №1,2 и 3 к процедуре «Р8-5 Запрос на изменение доступа к информационным системам и ресурсам компании».

2.4. ПОРЯДОК ИСПОЛЬЗОВАНИЯ СИСТЕМ КОНТРОЛЯ НА РАБОЧЕМ МЕСТЕ

В целях обеспечения информационной безопасности и рассмотрения её инцидентов, определен порядок использования систем контроля на рабочем месте, который определен в процедуре «Р8-_ Порядок использования систем контроля на рабочем месте».

2.5. РАБОТА ЗА ПРЕДЕЛАМИ КОМПАНИИ

ООО «МКК «ПРОФИРЕАЛ»
196084, Россия, Санкт-Петербург
Лиговский пр., дом 266, литера «О».
Тел.: +7 (812) 424 46 44
E-mail: info@profi-credit.ru, www.profi-credit.ru

2.5.1. Удаленное подключение сотрудников Компании

Для обеспечения работы вне офиса в Компании предусмотрен функционал удаленного подключения посредством S-Terra VPN Client к ресурсам Компании. Для получения данного доступа необходимо направить запрос в службу технической поддержки, подробнее процесс получения доступа описан в процедуре «Р8-5 Запрос доступа к информационным системам и ресурсам компании».
Сотрудники, которые работают удаленно от рабочего места, посредством подключения через защищенный канал VPN, обязуются соблюдать правила безопасной работы в сети для предотвращения утечки любой информации Компании, в том числе:

1. Обязательно следить за адресами, на которые ведут ссылки.
2. Перед вводом личной информации необходимо проверять адресную строку браузера, на предмет подозрительной ссылки:
   - строка ввода находится не на том же сайте, где находился пользователь;
   - в адресе изменена буква на похожую (mail.**ry**, yande**ks**.ru и подобные).
3. Запрещено переходить по незнакомым ссылкам, которые приходят на почту и другие средства коммуникации.
4. Запрещено скачивать неизвестные файлы, пришедшие на почту, даже если файл пришел от известного контакта.
5. Запрещено переходить по незнакомым ссылкам на подозрительные рекламные баннеры.
6. Не запускать программы для «взлома» (генераторы паролей, сетевые сканеры компьютеров, программы для очистки системы и т.д.).
7. Запрещено вставлять в компьютер любые съемные накопители (флэшки, внешние жесткие диски и.т.п.).

2.6. РАБОТА С ВНЕШНИМИ КОМПАНИЯМИ И ИСПОЛНИТЕЛЯМИ

2.6.1. Защита персональных данных

При работе с внешними компаниями и исполнителями необходимо удостовериться в безопасности канала передачи данных, через который осуществляется работа. Любая обработка (в том числе передача персональных данных) должна соответствовать Федеральному закону от 27.07.2006 №152-ФЗ «О персональных данных».

2.6.2. Способ организации обмена данными между Компанией и внешним исполнителем.

Для организации обмена данными между Компанией и внешним исполнителем должен быть направлен запрос через систему helpdesk руководителем отдела, которому необходимо организовать данный вид связи. В запросе должна быть указана информация:

- исполнитель, кому нужен удаленный доступ
- основания и цель доступа
- сроки предоставления доступа (с какого по какое число)
- описать ресурсы, необходимые для работы

ООО «МКК «ПРОФИРЕАЛ»
196084, Россия, Санкт-Петербург
Лиговский пр., дом 266, литера «О».
Тел.: +7 (812) 424 46 44
E-mail: info@profi-credit.ru, www.profi-credit.ru

- контакты ответственного лица за организацию обмена данными со стороны исполнителя.

Данный запрос должен быть согласован Специалистом по информационной безопасности или Директором отдела ИТ.
После окончания срока предоставления доступа, указанного в запросе, доступ отключается и руководителю отдела направляется извещение о данной операции.
Для изменения даты отключения канала обмена данными между Компанией и исполнителем руководитель отдела, с которым работает исполнитель, должен отправить запрос на helpdesk. В запросе должно быть указано обоснование и новый срок предоставления доступа.
При завершении работ с исполнителем раньше, чем установлена дата отключения доступа, необходимо уведомить об этом Специалиста по информационной безопасности или Директора по ИТ для принятия мер по отключению канала обмена данными.

2.7. РАЗГРАНИЧЕНИЕ ДОСТУПА В ИНТЕРНЕТ

2.7.1. Уровни доступа

В Компании существует разделение типов доступа в Интернет на 3 вида:

1. Разрешено все. Данный уровень не имеет ограничений к доступу в Интернет.
2. Разрешено все, кроме списка запрещенных Интернет ресурсов.
3. Запрещено все, кроме списка разрешенных Интернет ресурсов.

2.7.2. Группы пользователей

Отдел ИТ и Директора отделов имеют уровень доступа в Интернет 1 «Разрешено все».
Все сотрудники Компании имеют доступ в интернет с уровнем 2 «Разрешено все, кроме списка запрещенных ресурсов».
Группа с уровнем доступа 3 «Запрещено все, кроме списка разрешенных ресурсов» формируется по запросу от руководителей отделов и рассматривается Специалистом по ИБ.

2.7.3. Изменение уровня доступа к Интернету

Изменения доступа происходит согласно процедуре «Р8-5 Запрос на изменение доступа к информационным системам и ресурсам компании».

2.8. ПЕРЕДАЧА ПАРОЛЕЙ

2.8.1. Беспроводные точки доступа

Ввод паролей от беспроводных точек доступа производится сотрудниками отдела ИТ.
Запрещено передавать пароль от беспроводных точек доступа сотрудникам, не относящимся к отделу ИТ.

ООО «МКК «ПРОФИРЕАЛ»
196084, Россия, Санкт-Петербург
Лиговский пр., дом 266, литера «О».
Тел.: +7 (812) 424 46 44
E-mail: info@profi-credit.ru, www.profi-credit.ru

2.8.2. Пароли к информационным системам и ресурсам Компании

Запрещено передавать пароли третьим лицам к информационным системам и ресурсам Компании, которые использует сотрудник для выполнения своих служебных обязанностей.