

УТВЕРЖДАЮ
Директор ООО «Файнекс»


20.06.2023 А.А. Сташевский



ПОЛОЖЕНИЕ о назначении и распределении ролей в информационной системе ООО «Файнекс»

ГЛАВА 1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение о назначении и распределении ролей в информационной системе ООО «Файнекс» (далее – Положение) определяет принципы назначения и распределения ролей в ООО «Файнекс» (далее – Организация) для разграничения прав доступа пользователей к информационной системе Организации, а также к информационным ресурсам Организации, которые рассматриваются в качестве объектов защиты.

1.2. Для целей настоящего Положения нижеприведенные термины и сокращения используются в следующих значениях:

ДЛ ИБ – должностное лицо, ответственное за системное администрирование и информационную безопасность;

ДЛ ПВТ – должностное лицо, ответственное за соблюдение режима Парка высоких технологий;

ДЛ ПУР – должностное лицо, ответственное за управление рисками;

ИБ – информационная безопасность;

информационная система Организации (далее – ИС) – совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств, используемая Организацией для осуществления своей деятельности;

объект – аппаратное средство, программное средство, программно-аппаратное средство, информационный ресурс, услуга, процесс, система, над которыми выполняются действия;

ОДЛ ПОД/ФТ – ответственное должностное лицо в части выполнения требований по предотвращению легализации доходов, полученных преступным путем, финансирования террористической деятельности либо финансирования распространения оружия массового поражения

Политика ИБ – Политика информационной безопасности (кибербезопасности) ООО «Файнекс»;

полномочия – официально предоставленные возможности совершения над объектом каких-либо действий;

роль – заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом и объектом;

системный администратор – работник Организации, уполномоченный выполнять действия по обеспечению штатной работы персональных компьютеров, офисных серверов, сетевых коммуникаций, периферийного оборудования Организации;

субъект – лица из числа руководителей, сотрудников, клиентов Организации или иницилируемые от их имени процессы по выполнению действий над объектами.

1.3. Иные термины, применяемые в настоящем Положении, используются в значениях, определенных законодательством Республики Беларусь, актами Наблюдательного совета Парка высоких технологий (далее – ПВТ) и иными локальными правовыми актами Организации (далее – ЛПА).

1.4. В случаях, если отдельные нормы настоящего Положения противоречат законодательству Республики Беларусь, актам Наблюдательного совета ПВТ, данные нормы утрачивают силу и применяются соответствующие нормы законодательства Республики Беларусь, актов Наблюдательного совета ПВТ до внесения необходимых изменений в настоящее Положение. Недействительность отдельных норм Положения не влечет недействительность других норм Положения и Положения в целом.

1.5. Во всем ином, что не предусмотрено настоящим Положением, Организация руководствуется законодательством Республики Беларусь, актами Наблюдательного совета ПВТ и ЛПА.

ГЛАВА 2 РАСПРЕДЕЛЕНИЕ РОЛЕЙ

2.1. Роли применяются для объектов в целях предоставления доступа к ним только авторизованным работникам, т.е. работникам, которым необходимы права доступа к объектам для исполнения должностных обязанностей. Доступ ограничивается по принципу служебной необходимости. Предоставление доступа по принципу служебной необходимости означает предоставление работнику прав доступа, минимально необходимых и достаточных для выполнения им своих обязанностей.

2.2. Для каждой роли должны выделяться ресурсы объектов и определяться операции с ними, необходимые работнику для выполнения своих обязанностей в соответствии с назначенной ему ролью и в зависимости от исполняемых функций.

2.3. Возможные роли описываются в документации к объекту и выбираются из таблицы ролей (Приложение 1 к настоящему Положению).

2.4. Для эксплуатации объекта обязательны роли «Пользователь», «Администратор» и «Администратор ИБ».

2.5. Необходимость использования иных ролей зависит от типа и назначения объекта, не является обязательным и определяется в документации к объекту.

ГЛАВА 3 НАЗНАЧЕНИЕ РОЛЕЙ

3.1. Назначение ролей осуществляется ДЛ ИБ, в соответствии с Перечнем ролей в информационной системе ООО «Файнекс», представленным в Приложении 1 к настоящему Положению.

3.2. Допускается одновременное назначение работнику нескольких ролей для одного объекта с учетом Матрицы конфликтных ролей Организации, представленной в Приложении 2 к настоящему Положению. Исключение составляет совмещение работником сторонней организации ролей «Разработчик» и «Аудитор безопасности».

3.3. Контроль соответствия заявленных и фактически предоставленных ролей производится с периодичностью не реже одного раза в год, если иное не регламентируется в ЛПА и /или в документации к объекту, и осуществляется ДЛ ИБ.

3.4. В случае изменения занимаемой должности и/или функциональных обязанностей роли работника для каждого из объектов пересматриваются по процедуре, определенной в документации к объекту, и/или на основании приказа директора Организации.

3.5. Удаление ролей работника к любому объекту осуществляется работником Организации, которому назначена роль «Администратор ресурса», при увольнении работника на основании соответствующего приказа или выписки из данного приказа, в последний рабочий день увольняемого работника.

3.6. Временная блокировка ролей работника Организации к любому объекту осуществляется работником Организации, которому назначена роль «Администратор ресурса», по распоряжению ДЛ ИБ в случае возникновения инцидента ИБ, который регистрируется в соответствии с ЛПА по управлению рисками ИБ в Организации.

3.7. Восстановление ролей работника Организации к любому объекту при временной блокировке осуществляется работником Организации, которому назначена роль «Администратор ресурса», по распоряжению ДЛ ИБ (в случае, если временная блокировка была инициирована ДЛ ИБ), после проведения требуемых процедур по оценке и анализу произошедшего инцидента ИБ Организации и принятия мер по его недопущению в дальнейшем.

3.8. На время отсутствия работника его роли для каждого объекта могут быть назначены другому работнику.

Приложение 1
к Положению о назначении и
распределении ролей в информационной
системе ООО «Файнекс»

Перечень ролей в информационной системе ООО «Файнекс»

Наименование роли	Категории субъектов, которым может быть предоставлена роль с учетом Матрицы конфликтных ролей (Приложение 2)	Права доступа
Администратор ресурса	Директор, ДЛ ИБ, системный администратор	К средствам управления ресурсами объектов
Администратор ИБ	ДЛ ИБ	К средствам управления безопасностью объектов, в том числе средствам криптографической защиты информации и антивирусного программного обеспечения, включая средства аудита и анализа событий безопасности объектов
Аудитор безопасности	ДЛ ИБ, работники сторонних организаций (только для проведения внешнего аудита)	К объектам защиты и их средствам безопасности, необходимые для анализа рисков безопасности, анализа соответствия мер и средств безопасности, анализа эффективности Политики ИБ для обеспечения безопасности информационных технологий, используемых Организацией в своей деятельности
Пользователь	Работники Оператора (в соответствии с должностными обязанностями и Матрицей ролевого доступа (Приложение 3), работники сторонних организаций	К определенным ресурсам объектов, исходя из функционального назначения объектов и роли работника
Разработчик	Работники сторонних организаций	К объектам и их средствам безопасности только на период ввода объектов в эксплуатацию и период проведения модернизации, сопровождения

Приложение 2
к Положению о назначении и
распределении ролей в информационной
системе ООО «Файнекс»

Матрица конфликтных ролей в информационной системе ООО «Файнекс»

Роль	Директор	ДЛ ПВТ	ДЛ ПУР	ДЛ ИБ	ОДЛ ПОД/ФТ	Финансовая служба	Системный администратор	Служба поддержки
Директор								
ДЛ ПВТ								
ДЛ ПУР								
ДЛ ИБ								
ОДЛ ПОД/ФТ								
Финансовая служба								
Системный администратор								
Служба поддержки								

Приложение 3
к Положению о назначении и
распределении ролей в информационной
системе ООО «Файнекс»

Матрица ролевого доступа в информационной системе ООО «Файнекс»

Роль	Модуль API	Административный модуль	СУБД MariaDB	Модуль интеграции с COB	Портал	Сервер отчетов	Модуль мониторинга	Система управления кодом	Электронная почта	Интернет	Подключение к порту USB
Директор		X			X		X		X	X	X
ДЛ ПВТ					X		X		X	X	OD
ДЛ ПУР					X		X		X	X	OD
ДЛ ИБ	X	X	X	X	X	X	X	X	X	X	X
ОДЛ ПОД/ФТ		X			X		OD		X	X	OD
Финансовая служба		X			X		X		X	X	OD
Системный администратор	X	X	X	X	X	X	X	X	X	X	X
Служба поддержки		X			X		OD		X	X	OD

W	Запись	R	Чтение	OD	По согласованию с Директором и/или ДЛ ИБ
----------	--------	----------	--------	-----------	--