ПРОТОКОЛ № И-11/2014

заседания Совета
Некоммерческого партнерства «Объединение организаций выполняющих инженерные изыскания в газовой и нефтяной отрасли «Инженер-Изыскатель»

Место проведения заседания: г. Москва
Форма проведения – **очная**
Дата проведения заседания – 25 апреля 2014 года
Дата составления протокола – 25 апреля 2014 года

Присутствовали члены Совета Партнерства:
1. Скрепнюк Андрей Борисович
2. Азарх Михаил Михайлович
3. Алимов Сергей Викторович
4. Милованов Виктор Иванович
5. Небабин Владимир Викторович
6. Прозоров Сергей Фролович
7. Разумов Дмитрий Валерьевич
8. Савченков Сергей Викторович
9. Цыбульский Павел Геннадьевич
10. Шеховцов Андрей Викторович

В заседании приняли участие 10 членов Совета Партнерства из 11.
Кворум имеется.

Приглашенные:
1. Алексеев А.Б. – Заместитель директора НП «Инженер-Изыскатель»;
2. Иванов А.А. – Начальник Контрольно-экспертного отдела НП «Инженер-Изыскатель»;
3. Дрыгин Д.Ю. – Начальник Информационно-аналитического отдела НП «Инженер-Изыскатель»;
4. Рязанова В.Е. – Главный бухгалтер НП «Инженер-Изыскатель».

Председатель Совета **Некоммерческого партнерства «Объединение организаций выполняющих инженерные изыскания в газовой и нефтяной отрасли «Инженер-Изыскатель»** Скрепнюк Андрей Борисович.

Секретарь Совета **Некоммерческого партнерства «Объединение организаций выполняющих инженерные изыскания в газовой и нефтяной отрасли «Инженер-Изыскатель»** Дроганова Александра Александровна.

ПОВЕСТКА ДНЯ:

1. **О рассмотрении Концепции обеспечения безопасности сведений, предоставляемых членами Партнерства в электронном виде.**
2. **О рассмотрении проекта Правил контроля в области саморегулирования в новой редакции.**
3. **О рассмотрении Требований к сертификации систем менеджмента качества членов Партнерства в новой редакции.**

4. **Об утверждении состава Научно-технической комиссии Партнерства.**
5. **О рассмотрении годовой бухгалтерской отчетности Партнерства за 2013 год.**
6. **О рассмотрении Отчета Ревизионной комиссии Партнерства за 2013 год.**
7. **О выплате вознаграждений членам Ревизионной комиссии Партнерства.**
8. **О представлении кандидатов на должность членов Ревизионной комиссии Партнерства.**
9. **О рассмотрении Отчета Директора о финансово-хозяйственной деятельности Партнерства за 2013 год.**
10. **О рассмотрении Отчета Совета Партнерства за 2013 год.**
11. **О представлении кандидата в Совет Партнерства.**
12. **О представлении кандидата на должность Председателя Совета Партнерства.**
13. **О созыве годового Общего собрания членов Партнерства.**

По вопросу №1 повестки дня. О рассмотрении Концепции обеспечения безопасности сведений, предоставляемых членами Партнерства в электронном виде.

СЛУШАЛИ:
Дрыгина Д.Ю., который доложил о подготовке Концепции информационной безопасности Партнерства включающую в себя обеспечение безопасности сведений, предоставляемых членами Партнерства в электронном виде. Представил проект Концепции информационной безопасности Партнерства. Предложил одобрить Концепцию информационной безопасности Партнерства.

ВОПРОС, ПОСТАВЛЕННЫЙ НА ГОЛОСОВАНИЕ:
1.1. Одобрить Концепцию информационной безопасности Партнерства.

Голосовали:
Скрепнюк Андрей Борисович – «за»
Азарх Михаил Михайлович – «за»
Алимов Сергей Викторович – «за»
Милованов Виктор Иванович – «за»
Небабин Владимир Викторович – «за»
Прозоров Сергей Фролович – «за»
Разумов Дмитрий Валерьевич – «за»
Савченков Сергей Викторович – «за»
Цыбульский Павел Геннадьевич – «за»
Шеховцов Андрей Викторович – «за»

«за» - десять голосов, «против» - нет, «воздержался» - нет.
Решение принято.

РЕШИЛИ:
1.1. Одобрить Концепцию информационной безопасности Партнерства.

По вопросу №2 повестки дня. О рассмотрении проекта Правил контроля в области саморегулирования в новой редакции.

СЛУШАЛИ:
Иванова А.А., который сообщил, что Партнерством разработан проект Правил контроля в области саморегулирования в новой редакции с целью приведения их в соответствие с внутренними документами Партнерства.
Предложил одобрить проект Правил контроля в области саморегулирования в новой редакции, представить его на утверждение Общему собранию членов Партнерства и рекомендовать Общему собранию членов Партнерства утвердить Правила контроля в области саморегулирования в новой редакции.

ВОПРОСЫ, ПОСТАВЛЕННЫЕ НА ГОЛОСОВАНИЕ:
2.1. Одобрить и представить на утверждение Общему собранию членов Партнерства проект Правил контроля в области саморегулирования в новой редакции.
2.2. Рекомендовать Общему собранию членов Партнерства утвердить Правила контроля в области саморегулирования в новой редакции.

Голосовали:
Скрепнюк Андрей Борисович – «за»
Азарх Михаил Михайлович – «за»
Алимов Сергей Викторович – «за»
Милованов Виктор Иванович – «за»
Небабин Владимир Викторович – «за»
Прозоров Сергей Фролович – «за»
Разумов Дмитрий Валерьевич – «за»
Савченков Сергей Викторович – «за»
Цыбульский Павел Геннадьевич – «за»
Шеховцов Андрей Викторович – «за»

«за» - десять голосов, «против» - нет, «воздержался» - нет.
Решение принято.

РЕШИЛИ:
2.1. Одобрить и представить на утверждение Общему собранию членов Партнерства проект Правил контроля в области саморегулирования в новой редакции.
2.2. Рекомендовать Общему собранию членов Партнерства утвердить Правила контроля в области саморегулирования в новой редакции.

По вопросу №3 повестки дня. О рассмотрении Требований к сертификации систем менеджмента качества членов Партнерства в новой редакции.

СЛУШАЛИ:
Иванова А.А., который сообщил о необходимости пересмотра Требований к сертификации систем менеджмента качества членов Партнерства в новой редакции и представил проект Требований. Предложил одобрить представленный проект Требований и рекомендовать Общему собранию членов Партнерства утвердить Требования к сертификации систем менеджмента качества членов Партнерства в новой редакции.

ВОПРОСЫ, ПОСТАВЛЕННЫЕ НА ГОЛОСОВАНИЕ:
3.1. Одобрить проект Требований к сертификации систем менеджмента качества членов Партнерства в новой редакции.
3.2. Рекомендовать Общему собранию членов Партнерства утвердить Требования к сертификации систем менеджмента качества членов Партнерства в новой редакции.

Голосовали:
Скрепнюк Андрей Борисович – «за»
Азарх Михаил Михайлович – «за»
Алимов Сергей Викторович – «за»
Милованов Виктор Иванович – «за»
Небабин Владимир Викторович – «за»
Прозоров Сергей Фролович – «за»
Разумов Дмитрий Валерьевич – «за»
Савченков Сергей Викторович – «за»
Цыбульский Павел Геннадьевич – «за»
Шеховцов Андрей Викторович – «за»

«за» - десять голосов, «против» - нет, «воздержался» - нет.
Решение принято.

РЕШИЛИ:
3.1. Одобрить проект Требований к сертификации систем менеджмента качества членов Партнерства в новой редакции.
3.2. Рекомендовать Общему собранию членов Партнерства утвердить Требования к сертификации систем менеджмента качества членов Партнерства в новой редакции.

По вопросу №4 повестки дня. Об утверждении состава Научно-технической комиссии Партнерства.

СЛУШАЛИ:
Алексеева А.Б., который сообщил, что на основании решения Совета Партнерства (Протокол заседания Совета Партнерства № И-02/2014 от 29.01.2014 г.) Партнерством подготовлены предложения по составу Научно-технической комиссии Партнерства.
Предложил утвердить следующий состав Комиссии:
1) Азарх Михаил Михайлович - Председатель;
2) Липилин Владимир Александрович;
3) Миронюк Сергей Григорьевич;
4) Задорожный Сергей Петрович;
5) Зазерин Андрей Иванович.

ВОПРОС, ПОСТАВЛЕННЫЙ НА ГОЛОСОВАНИЕ:
4.1. Утвердить состав Научно-технической комиссии Партнерства:
1) Азарх Михаил Михайлович - Председатель;
2) Липилин Владимир Александрович;
3) Миронюк Сергей Григорьевич;
4) Задорожный Сергей Петрович;
5) Зазерин Андрей Иванович.

Голосовали:
Скрепнюк Андрей Борисович – «за»
Азарх Михаил Михайлович – «за»
Алимов Сергей Викторович – «за»
Милованов Виктор Иванович – «за»
Небабин Владимир Викторович – «за»
Прозоров Сергей Фролович – «за»
Разумов Дмитрий Валерьевич – «за»

Савченков Сергей Викторович – «за»
Цыбульский Павел Геннадьевич – «за»
Шеховцов Андрей Викторович – «за»

«за» - десять голосов, «против» - нет, «воздержался» - нет.
Решение принято.

РЕШИЛИ:
4.1. Утвердить состав Научно-технической комиссии Партнерства:

1) **Азарх Михаил Михайлович - Председатель;**
2) **Липилин Владимир Александрович;**
3) **Миронюк Сергей Григорьевич;**
4) **Задорожный Сергей Петрович;**
5) **Зазерин Андрей Иванович.**

По вопросу №5 повестки дня. О рассмотрении годовой бухгалтерской отчетности Партнерства за 2013 год.

СЛУШАЛИ:
Рязанову В.Е., которая представила годовую бухгалтерскую отчетность Партнерства за 2013 год. Предложила рекомендовать Общему собранию членов Партнерства утвердить годовую бухгалтерскую отчетность Партнерства за 2013 год.

ВОПРОС, ПОСТАВЛЕННЫЙ НА ГОЛОСОВАНИЕ:
5.1. Принять к сведению годовую бухгалтерскую отчетность Партнерства за 2013 год и рекомендовать Общему собранию членов Партнерства утвердить годовую бухгалтерскую отчетность Партнерства за 2013 год.

Голосовали:
Скрепнюк Андрей Борисович – «за»
Азарх Михаил Михайлович – «за»
Алимов Сергей Викторович – «за»
Милованов Виктор Иванович – «за»
Небабин Владимир Викторович – «за»
Прозоров Сергей Фролович – «за»
Разумов Дмитрий Валерьевич – «за»
Савченков Сергей Викторович – «за»
Цыбульский Павел Геннадьевич – «за»
Шеховцов Андрей Викторович – «за»

«за» - десять голосов, «против» - нет, «воздержался» - нет.
Решение принято.

РЕШИЛИ:
5.1. Принять к сведению годовую бухгалтерскую отчетность Партнерства за 2013 год и рекомендовать Общему собранию членов Партнерства утвердить годовую бухгалтерскую отчетность Партнерства за 2013 год.

По вопросу №6 повестки дня. О рассмотрении Отчета Ревизионной комиссии Партнерства за 2013 год.

СЛУШАЛИ:
Алексеева А.Б., который доложил, что Ревизионной комиссией Партнерства проведена проверка финансово-хозяйственной и правовой деятельности Партнерства за 2013 год, представил на рассмотрение Совету Партнерства Отчет Ревизионной комиссии Партнерства за 2013 год.

ВОПРОС, ПОСТАВЛЕННЫЙ НА ГОЛОСОВАНИЕ:
6.1. Принять к сведению Отчет Ревизионной комиссии Партнерства за 2013 год.

Голосовали:
Скрепнюк Андрей Борисович – «за»
Азарх Михаил Михайлович – «за»
Алимов Сергей Викторович – «за»
Милованов Виктор Иванович – «за»
Небабин Владимир Викторович – «за»
Прозоров Сергей Фролович – «за»
Разумов Дмитрий Валерьевич – «за»
Савченков Сергей Викторович – «за»
Цыбульский Павел Геннадьевич – «за»
Шеховцов Андрей Викторович – «за»

«за» - десять голосов, «против» - нет, «воздержался» - нет.
Решение принято.

РЕШИЛИ:
6.1. Принять к сведению Отчет Ревизионной комиссии Партнерства за 2013 год.

По вопросу №7 повестки дня. О выплате вознаграждений членам Ревизионной комиссии Партнерства.

СЛУШАЛИ:
Скрепнюка А.Б., который отметил удовлетворительную работу Ревизионной комиссии Партнерства в 2013 году и предложил рекомендовать Общему собранию членов Партнерства принять решение о выплате вознаграждений членам Ревизионной комиссии Партнерства по итогам работы в 2013 году в следующем размере:

1. Фомина Людмила Павловна – 80 000 (восемьдесят тысяч) рублей 00 копеек;
2. Полякова Ольга Владимировна – 40 000 (сорок тысяч) рублей 00 копеек;
3. Лабецкая Любовь Федоровна – 40 000 (сорок тысяч) рублей 00 копеек.

ВОПРОС, ПОСТАВЛЕННЫЙ НА ГОЛОСОВАНИЕ:
7.1. Рекомендовать Общему собранию членов Партнерства принять решение о выплате вознаграждений членам Ревизионной комиссии Партнерства по итогам работы в 2013 году в следующем размере:

1. Фомина Людмила Павловна – 80 000 (восемьдесят тысяч) рублей 00 копеек;
2. Полякова Ольга Владимировна – 40 000 (сорок тысяч) рублей 00 копеек;
3. Лабецкая Любовь Федоровна – 40 000 (сорок тысяч) рублей 00 копеек.

Голосовали:
Скрепнюк Андрей Борисович – «за»
Азарх Михаил Михайлович – «за»
Алимов Сергей Викторович – «за»
Милованов Виктор Иванович – «за»

Небабин Владимир Викторович – «за»
Прозоров Сергей Фролович – «за»
Разумов Дмитрий Валерьевич – «за»
Савченков Сергей Викторович – «за»
Цыбульский Павел Геннадьевич – «за»
Шеховцов Андрей Викторович – «за»

«за» - десять голосов, «против» - нет, «воздержался» - нет.
Решение принято.

РЕШИЛИ:
7.1. Рекомендовать Общему собранию членов Партнерства принять решение о выплате вознаграждений членам Ревизионной комиссии Партнерства по итогам работы в 2013 году в следующем размере:

1. **Фомина Людмила Павловна – 80 000 (восемьдесят тысяч) рублей 00 копеек;**
2. **Полякова Ольга Владимировна – 40 000 (сорок тысяч) рублей 00 копеек;**
3. **Лабецкая Любовь Федоровна – 40 000 (сорок тысяч) рублей 00 копеек.**

По вопросу №8 повестки дня. О представлении кандидатов на должность членов Ревизионной комиссии Партнерства.

СЛУШАЛИ:
Алексеева А.Б., который доложил, что срок полномочий Ревизионной комиссии Партнерства истекает 27 июня 2014 года (Протокол Общего собрания членов Партнерства № 9 от 27.06.2012 г.). Отметил, что в соответствии с п. 9.10.5 Устава Партнерства в компетенцию Совета Партнерства входит представление Общему собранию членов Партнерства кандидатов для назначения на должность членов Ревизионной комиссии Партнерства. Сообщил, что Партнерством получено письмо от члена Партнерства ОАО «Фундаментпроект» с предложением включить в Ревизионную комиссию Партнерства своего представителя Заместителя директора по экономическим вопросам - Главного бухгалтера Салькова Николая Петровича.
Скрепнюка А.Б., который предложил, учитывая положительный опыт работы ранее избранных членов Ревизионной комиссии Партнерства, а также поступившее предложение от члена Партнерства, рекомендовать Общему собранию членов Партнерства избрать Ревизионную комиссию Партнерства в следующем составе:

1. Фомина Людмила Павловна;
2. Полякова Ольга Владимировна;
3. Сальков Николай Петрович.

ВОПРОС, ПОСТАВЛЕННЫЙ НА ГОЛОСОВАНИЕ:
8.1. Рекомендовать Общему собранию членов Партнерства избрать Ревизионную комиссию Партнерства в следующем составе:

1. Фомина Людмила Павловна;
2. Полякова Ольга Владимировна;
3. Сальков Николай Петрович.

Голосовали:
Скрепнюк Андрей Борисович – «за»
Азарх Михаил Михайлович – «за»
Алимов Сергей Викторович – «за»
Милованов Виктор Иванович – «за»
Небабин Владимир Викторович – «за»
Прозоров Сергей Фролович – «за»

Разумов Дмитрий Валерьевич – «за»
Савченков Сергей Викторович – «за»
Цыбульский Павел Геннадьевич – «за»
Шеховцов Андрей Викторович – «за»

«за» - десять голосов, «против» - нет, «воздержался» - нет.
Решение принято.

РЕШИЛИ:
8.1. Рекомендовать Общему собранию членов Партнерства избрать Ревизионную комиссию Партнерства в следующем составе:

1. **Фомина Людмила Павловна;**
2. **Полякова Ольга Владимировна;**
3. **Салькoв Николай Петрович.**

По вопросу №9 повестки дня. О рассмотрении Отчета Директора о финансово-хозяйственной Партнерства за 2013 год.

СЛУШАЛИ:
Азарха М.М., который представил Отчет Директора о финансово-хозяйственной деятельности Партнерства за 2013 год. Предложил одобрить представленный Отчет и рекомендовать Общему собранию членов Партнерства утвердить Отчет Директора о финансово-хозяйственной деятельности Партнерства за 2013 год.

ВОПРОСЫ, ПОСТАВЛЕННЫЕ НА ГОЛОСОВАНИЕ:
9.1. Одобрить Отчет Директора о финансово-хозяйственной деятельности Партнерства за 2013 год.
9.2. Рекомендовать Общему собранию членов Партнерства утвердить Отчет Директора о финансово-хозяйственной деятельности Партнерства за 2013 год.

Голосовали:
Скрепнюк Андрей Борисович – «за»
Азарх Михаил Михайлович – «за»
Алимов Сергей Викторович – «за»
Милованов Виктор Иванович – «за»
Небабин Владимир Викторович – «за»
Прозоров Сергей Фролович – «за»
Разумов Дмитрий Валерьевич – «за»
Савченков Сергей Викторович – «за»
Цыбульский Павел Геннадьевич – «за»
Шеховцов Андрей Викторович – «за»

«за» - десять голосов, «против» - нет, «воздержался» - нет.
Решение принято.

РЕШИЛИ:
9.1. Одобрить Отчет Директора о финансово-хозяйственной деятельности Партнерства за 2013 год.
9.2. Рекомендовать Общему собранию членов Партнерства утвердить Отчет Директора о финансово-хозяйственной деятельности Партнерства за 2013 год.

По вопросу №10 повестки дня. О рассмотрении Отчета Совета Партнерства за 2013 год.

СЛУШАЛИ:
Дроганову А.А., которая представила Отчет Совета Партнерства за 2013 год. Предложила одобрить представленный Отчет и рекомендовать Общему собранию членов Партнерства утвердить Отчет Совета Партнерства за 2013 год.

ВОПРОСЫ, ПОСТАВЛЕННЫЕ НА ГОЛОСОВАНИЕ:
10.1. Одобрить Отчет Совета Партнерства за 2013 год.
10.2. Рекомендовать Общему собранию членов Партнерства утвердить Отчет Совета Партнерства за 2013 год.

Голосовали:
Скрепнюк Андрей Борисович – «за»
Азарх Михаил Михайлович – «за»
Алимов Сергей Викторович – «за»
Милованов Виктор Иванович – «за»
Небабин Владимир Викторович – «за»
Прозоров Сергей Фролович – «за»
Разумов Дмитрий Валерьевич – «за»
Савченков Сергей Викторович – «за»
Цыбульский Павел Геннадьевич – «за»
Шеховцов Андрей Викторович – «за»

«за» - десять голосов, «против» - нет, «воздержался» - нет.
Решение принято.

РЕШИЛИ:
10.1. Одобрить Отчет Совета Партнерства за 2013 год.
10.2. Рекомендовать Общему собранию членов Партнерства утвердить Отчет Совета Партнерства за 2013 год.

По вопросу №11 повестки дня. О представлении кандидата в Совет Партнерства.

СЛУШАЛИ:
Скрепнюка А.Б., который сообщил о поступлении заявления Гафарова Наиля Анатольевича о досрочном сложении с себя полномочий члена Совета Партнерства и просьбой вынести вопрос о досрочном прекращении его полномочий в качестве члена Совета Партнерства на ближайшее Общее собрание членов Партнерства.
Азарха М.М., который сообщил, что в адрес Партнерства поступило предложение от члена Партнерства ОАО «СевКавНИПИгаз» о выдвижении кандидатуры Минликаева Валерия Зиряковича в Совет Партнерства.
Письменное согласие кандидата представлено.
Предложил включить представленную кандидатуру в список кандидатов для избрания в Совет Партнерства на Общем собрании членов Партнерства.
Доложил, что в соответствии с п. 9.10.5 Устава Партнерства в компетенцию Совета Партнерства входит представление Общему собранию членов Партнерства кандидатов в Совет Партнерства.
Скрепнюка А.Б., который предложил вынести вопрос о досрочном прекращении полномочий Гафарова Наиля Анатольевича в качестве члена Совета Партнерства на Общее собрание членов Партнерства и представить Общему собранию членов Партнерства кандидатуру Минликаева Валерия Зиряковича для избрания в Совет

Партнерства, а также рекомендовать Общему собранию членов Партнерства определить срок полномочий вновь избранного члена Совета Партнерства до момента прекращения срока полномочий ранее избранного состава Совета Партнерства (Протокол Общего собрания членов Партнерства № 10 от 11.10.2012 г.).

ВОПРОСЫ, ПОСТАВЛЕННЫЕ НА ГОЛОСОВАНИЕ:

11.1. Рекомендовать Общему собранию членов Партнерства досрочно прекратить полномочия Гафарова Наиля Анатольевича в качестве члена Совета Партнерства.

11.2. Включить Минликаева Валерия Зиряковича в список кандидатов для избрания в Совет Партнерства на Общем собрании членов Партнерства.

11.3. Представить Общему собранию членов Партнерства кандидатуру Минликаева Валерия Зиряковича для избрания в Совет Партнерства.

11.4. Рекомендовать Общему собранию членов Партнерства определить срок полномочий вновь избранного члена Совета Партнерства до момента прекращения срока полномочий ранее избранного состава Совета Партнерства.

Голосовали:
Скрепнюк Андрей Борисович – «за»
Азарх Михаил Михайлович – «за»
Алимов Сергей Викторович – «за»
Милованов Виктор Иванович – «за»
Небабин Владимир Викторович – «за»
Прозоров Сергей Фролович – «за»
Разумов Дмитрий Валерьевич – «за»
Савченков Сергей Викторович – «за»
Цыбульский Павел Геннадьевич – «за»
Шеховцов Андрей Викторович – «за»

«за» - десять голосов, «против» - нет, «воздержался» - нет.
Решение принято.

РЕШИЛИ:

11.1. Рекомендовать Общему собранию членов Партнерства досрочно прекратить полномочия Гафарова Наиля Анатольевича в качестве члена Совета Партнерства.

11.2. Включить Минликаева Валерия Зиряковича в список кандидатов для избрания в Совет Партнерства на Общем собрании членов Партнерства.

11.3. Представить Общему собранию членов Партнерства кандидатуру Минликаева Валерия Зиряковича для избрания в Совет Партнерства.

11.4. Рекомендовать Общему собранию членов Партнерства определить срок полномочий вновь избранного члена Совета Партнерства до момента прекращения срока полномочий ранее избранного состава Совета Партнерства.

По вопросу №12 повестки дня. О представлении кандидата на должность Председателя Совета Партнерства.

СЛУШАЛИ:

Азарха М.М., который отметил, что существенное положительное влияние на развитие Партнерства оказали знания, практический опыт и умелое руководство Председателя Совета Партнерства Скрепнюка Андрея Борисовича.

Сообщил, руководствуясь решением Общего собрания членов Партнерства (Протокол № 10 от 11.10.2012 г.), что полномочия Скрепнюка Андрея Борисовича в качестве Председателя Совета Партнерства прекращаются 26.11.2014 г. Отметил, что в соответствии с п. 9.10.5 Устава Партнерства в компетенцию Совета Партнерства

входит представление Общему собранию членов Партнерства кандидата для назначения на должность Председателя Совета Партнерства.
Предложил представить Общему собранию членов Партнерства кандидатуру Скрепнюка Андрея Борисовича для назначения на должность Председателя Совета Партнерства с 27.11.2014 г. на новый срок согласно п. 9.13 Устава Партнерства.

ВОПРОС, ПОСТАВЛЕННЫЙ НА ГОЛОСОВАНИЕ:
12.1. Представить Общему собранию членов Партнерства кандидатуру Скрепнюка Андрея Борисовича для назначения на должность Председателя Совета Партнерства с 27.11.2014 г. на новый срок согласно п. 9.13 Устава Партнерства.

Голосовали:
Азарх Михаил Михайлович – «за»
Алимов Сергей Викторович – «за»
Милованов Виктор Иванович – «за»
Небабин Владимир Викторович – «за»
Прозоров Сергей Фролович – «за»
Разумов Дмитрий Валерьевич – «за»
Савченков Сергей Викторович – «за»
Цыбульский Павел Геннадьевич – «за»
Шеховцов Андрей Викторович – «за»

Скрепнюк Андрей Борисович не принимал участие в голосовании по вопросу в соответствии со ст. 8 «Заинтересованные лица. Конфликт интересов» Федерального закона «О саморегулируемых организациях» от 01.12.2007 г. № 315-ФЗ.

«за» - девять голосов, «против» - нет, «воздержался» - нет.
Решение принято.

РЕШИЛИ:
12.1. Представить Общему собранию членов Партнерства кандидатуру Скрепнюка Андрея Борисовича для назначения на должность Председателя Совета Партнерства с 27.11.2014 г. на новый срок согласно п. 9.13 Устава Партнерства.

По вопросу №13 повестки дня. О созыве годового Общего собрания членов Партнерства.

СЛУШАЛИ:
Скрепнюка А.Б., который предложил:
13.1. Созвать годовое Общее собрание членов Партнерства.
13.2. Провести годовое Общее собрание членов Партнерства путем совместного присутствия членов Партнерства для обсуждения вопросов повестки дня и принятия решений по вопросам повестки дня, поставленным на голосование.
13.3. Установить дату, место и время проведения годового Общего собрания членов Партнерства:
- дата проведения: 28 мая 2014 года;
- место проведения: г. Москва, ул. Новый Арбат, д. 36/9, Здание Правительства Москвы, большой зал.
- время открытия собрания 14 часов 00 минут.
13.4. Установить дату, место и время начала регистрации участников годового Общего собрания членов Партнерства: 28 мая 2014 года, 13 часов 00 минут, по адресу: г. Москва, ул. Новый Арбат, д. 36/9, Здание Правительства Москвы, большой зал.

13.5. Утвердить повестку дня годового Общего собрания членов Партнерства:

1) Об утверждении Отчета Совета Партнерства за 2013 год.
2) Об утверждении Отчета Директора о финансово-хозяйственной деятельности Партнерства в 2013 году.
3) Об утверждении годовой бухгалтерской отчетности Партнерства за 2013 год.
4) Об утверждении Сметы Партнерства на 2014 год.
5) Об утверждении Требований к сертификации систем менеджмента качества членов Партнерства в новой редакции.
6) Об утверждении Положения о предоставлении информации о своей деятельности членами Партнерства в Партнерство в новой редакции.
7) Об утверждении Правил контроля в области саморегулирования в новой редакции.
8) О выплате вознаграждений членам Ревизионной комиссии Партнерства по итогам работы в 2013 году.
9) Об избрании Ревизионной комиссии Партнерства.
10) О внесении изменений в состав Совета Партнерства.
11) Об избрании Председателя Совета Партнерства.

13.6. Утвердить перечень информации (материалов), предоставляемой членам Партнерства при подготовке к проведению годового Общего собрания членов Партнерства:

1) Отчет Совета Партнерства за 2013 год.
2) Отчет Директора о финансово-хозяйственной деятельности Партнерства в 2013 году.
3) Годовая бухгалтерская отчетность Партнерства за 2013 г.
4) Проект Сметы Партнерства на 2014 год.
5) Проект Требований к сертификации систем менеджмента качества членов Партнерства в новой редакции.
6) Проект Положения о предоставлении информации о своей деятельности членами Партнерства в Партнерство в новой редакции.
7) Проект Правил контроля в области саморегулирования в новой редакции.
8) Рекомендации Совета Партнерства по вопросу 8 повестки дня годового Общего собрания членов Партнерства.
9) Рекомендации Совета Партнерства по вопросу 9 повестки дня годового Общего собрания членов Партнерства.
10) Рекомендации Совета Партнерства по вопросу 10 повестки дня годового Общего собрания членов Партнерства.
11) Рекомендации Совета Партнерства по вопросу 11 повестки дня годового Общего собрания членов Партнерства.
12) Отчет Ревизионной комиссии Партнерства в 2013 году.

13.7. Определить, что с информацией (материалами), предоставляемой членам Партнерства при подготовке к проведению годового Общего собрания членов Партнерства, можно ознакомиться с 28 апреля 2014 года по адресу: 125367, г. Москва, ул. Габричевского, д. 5, корп. 1 с понедельника по пятницу с 09 часов 00 минут до 17 часов 00 минут, а также на сайте Партнерства http://www.izsro.ru/.

13.8. Определить следующий порядок уведомления о проведении годового Общего собрания членов Партнерства: письменное сообщение о проведении годового Общего собрания членов Партнерства направляется не позднее, чем за 30 дней до даты проведения годового Общего собрания членов Партнерства, каждому члену Партнерства заказным письмом по адресу, указанному в реестре членов Партнерства, или вручается лично под роспись, а также сообщение о проведении годового Общего собрания членов

Партнерства и информация (материалы), предоставляемая членам Партнерства при подготовке к проведению годового Общего собрания членов Партнерства, размещаются на сайте Партнерства http://www.izsro.ru/.

13.9. Утвердить текст Сообщения о проведении годового Общего собрания членов Партнерства (Приложение № 1).

13.10. Утвердить формы бюллетеней для голосования по вопросам повестки дня годового Общего собрания членов Партнерства (Приложение № 2).

ВОПРОСЫ, ПОСТАВЛЕННЫЕ НА ГОЛОСОВАНИЕ:

13.1. Созвать годовое Общее собрание членов Партнерства.

13.2. Провести годовое Общее собрание членов Партнерства путем совместного присутствия членов Партнерства для обсуждения вопросов повестки дня и принятия решений по вопросам повестки дня, поставленным на голосование.

13.3. Установить дату, место и время проведения годового Общего собрания членов Партнерства:

- дата проведения: 28 мая 2014 года;
- место проведения: г. Москва, ул. Новый Арбат, д. 36/9, Здание Правительства Москвы, большой зал.
- время открытия собрания 14 часов 00 минут.

13.4. Установить дату, место и время начала регистрации участников годового Общего собрания членов Партнерства: 28 мая 2014 года, 13 часов 00 минут, по адресу: г. Москва, ул. Новый Арбат, д. 36/9, Здание Правительства Москвы, большой зал.

13.5. Утвердить повестку дня годового Общего собрания членов Партнерства:

1) Об утверждении Отчета Совета Партнерства за 2013 год.
2) Об утверждении Отчета Директора о финансово-хозяйственной деятельности Партнерства в 2013 году.
3) Об утверждении годовой бухгалтерской отчетности Партнерства за 2013 год.
4) Об утверждении Сметы Партнерства на 2014 год.
5) Об утверждении Требований к сертификации систем менеджмента качества членов Партнерства в новой редакции.
6) Об утверждении Положения о предоставлении информации о своей деятельности членами Партнерства в Партнерство в новой редакции.
7) Об утверждении Правил контроля в области саморегулирования в новой редакции.
8) О выплате вознаграждений членам Ревизионной комиссии Партнерства по итогам работы в 2013 году.
9) Об избрании Ревизионной комиссии Партнерства.
10) О внесении изменений в состав Совета Партнерства.
11) Об избрании Председателя Совета Партнерства.

13.6. Утвердить перечень информации (материалов), предоставляемой членам Партнерства при подготовке к проведению годового Общего собрания членов Партнерства:

1) Отчет Совета Партнерства за 2013 год.
2) Отчет Директора о финансово-хозяйственной деятельности Партнерства в 2013 году.
3) Годовая бухгалтерская отчетность Партнерства за 2013 г.
4) Проект Сметы Партнерства на 2014 год.
5) Проект Требований к сертификации систем менеджмента качества членов Партнерства в новой редакции.

6) Проект Положения о предоставлении информации о своей деятельности членами Партнерства в Партнерство в новой редакции.
7) Проект Правил контроля в области саморегулирования в новой редакции.
8) Рекомендации Совета Партнерства по вопросу 8 повестки дня годового Общего собрания членов Партнерства.
9) Рекомендации Совета Партнерства по вопросу 9 повестки дня годового Общего собрания членов Партнерства.
10) Рекомендации Совета Партнерства по вопросу 10 повестки дня годового Общего собрания членов Партнерства.
11) Рекомендации Совета Партнерства по вопросу 11 повестки дня годового Общего собрания членов Партнерства.
12) Отчет Ревизионной комиссии Партнерства в 2013 году.

13.7. Определить, что с информацией (материалами), предоставляемой членам Партнерства при подготовке к проведению годового Общего собрания членов Партнерства, можно ознакомиться с 28 апреля 2014 года по адресу: 125367, г. Москва, ул. Габричевского, д. 5, корп. 1 с понедельника по пятницу с 09 часов 00 минут до 17 часов 00 минут, а также на сайте Партнерства http://www.izsro.ru/.

13.8. Определить следующий порядок уведомления о проведении годового Общего собрания членов Партнерства: письменное сообщение о проведении годового Общего собрания членов Партнерства направляется не позднее, чем за 30 дней до даты проведения годового Общего собрания членов Партнерства, каждому члену Партнерства заказным письмом по адресу, указанному в реестре членов Партнерства, или вручается лично под роспись, а также сообщение о проведении годового Общего собрания членов Партнерства и информация (материалы), предоставляемая членам Партнерства при подготовке к проведению годового Общего собрания членов Партнерства, размещаются на сайте Партнерства http://www.izsro.ru/.

13.9. Утвердить текст Сообщения о проведении годового Общего собрания членов Партнерства (Приложение № 1).

13.10. Утвердить формы бюллетеней для голосования по вопросам повестки дня годового Общего собрания членов Партнерства (Приложение № 2).

Голосовали:
Скрепнюк Андрей Борисович – «за»
Азарх Михаил Михайлович – «за»
Алимов Сергей Викторович – «за»
Милованов Виктор Иванович – «за»
Небабин Владимир Викторович – «за»
Прозоров Сергей Фролович – «за»
Разумов Дмитрий Валерьевич – «за»
Савченков Сергей Викторович – «за»
Цыбульский Павел Геннадьевич – «за»
Шеховцов Андрей Викторович – «за»

«за» - десять голосов, «против» - нет, «воздержался» - нет.
Решение принято.

РЕШИЛИ:
13.1. Созвать годовое Общее собрание членов Партнерства.

13.2. Провести годовое Общее собрание членов Партнерства путем совместного присутствия членов Партнерства для обсуждения вопросов повестки дня и принятия решений по вопросам повестки дня, поставленным на голосование.

13.3. Установить дату, место и время проведения годового Общего собрания членов Партнерства:

- дата проведения: 28 мая 2014 года;

- место проведения: г. Москва, ул. Новый Арбат, д. 36/9, Здание Правительства Москвы, большой зал.

- время открытия собрания 14 часов 00 минут.

13.4. Установить дату, место и время начала регистрации участников годового Общего собрания членов Партнерства: 28 мая 2014 года, 13 часов 00 минут, по адресу: г. Москва, ул. Новый Арбат, д. 36/9, Здание Правительства Москвы, большой зал.

13.5. Утвердить повестку дня годового Общего собрания членов Партнерства:

1) **Об утверждении Отчета Совета Партнерства за 2013 год.**
2) **Об утверждении Отчета Директора о финансово-хозяйственной деятельности Партнерства в 2013 году.**
3) **Об утверждении годовой бухгалтерской отчетности Партнерства за 2013 год.**
4) **Об утверждении Сметы Партнерства на 2014 год.**
5) **Об утверждении Требований к сертификации систем менеджмента качества членов Партнерства в новой редакции.**
6) **Об утверждении Положения о предоставлении информации о своей деятельности членами Партнерства в Партнерство в новой редакции.**
7) **Об утверждении Правил контроля в области саморегулирования в новой редакции.**
8) **О выплате вознаграждений членам Ревизионной комиссии Партнерства по итогам работы в 2013 году.**
9) **Об избрании Ревизионной комиссии Партнерства.**
10) **О внесении изменений в состав Совета Партнерства.**
11) **Об избрании Председателя Совета Партнерства.**

13.6. Утвердить перечень информации (материалов), предоставляемой членам Партнерства при подготовке к проведению годового Общего собрания членов Партнерства:

1) **Отчет Совета Партнерства за 2013 год.**
2) **Отчет Директора о финансово-хозяйственной деятельности Партнерства в 2013 году.**
3) **Годовая бухгалтерская отчетность Партнерства за 2013 г.**
4) **Проект Сметы Партнерства на 2014 год.**
5) **Проект Требований к сертификации систем менеджмента качества членов Партнерства в новой редакции.**
6) **Проект Положения о предоставлении информации о своей деятельности членами Партнерства в Партнерство в новой редакции.**
7) **Проект Правил контроля в области саморегулирования в новой редакции.**
8) **Рекомендации Совета Партнерства по вопросу 8 повестки дня годового Общего собрания членов Партнерства.**
9) **Рекомендации Совета Партнерства по вопросу 9 повестки дня годового Общего собрания членов Партнерства.**
10) **Рекомендации Совета Партнерства по вопросу 10 повестки дня годового Общего собрания членов Партнерства.**

11) **Рекомендации Совета Партнерства по вопросу 11 повестки дня годового Общего собрания членов Партнерства.**
12) **Отчет Ревизионной комиссии Партнерства в 2013 году.**

13.7. Определить, что с информацией (материалами), предоставляемой членам Партнерства при подготовке к проведению годового Общего собрания членов Партнерства, можно ознакомиться с 28 апреля 2014 года по адресу: 125367, г. Москва, ул. Габричевского, д. 5, корп. 1 с понедельника по пятницу с 09 часов 00 минут до 17 часов 00 минут, а также на сайте Партнерства http://www.izsro.ru/.

13.8. Определить следующий порядок уведомления о проведении годового Общего собрания членов Партнерства: письменное сообщение о проведении годового Общего собрания членов Партнерства направляется не позднее, чем за 30 дней до даты проведения годового Общего собрания членов Партнерства, каждому члену Партнерства заказным письмом по адресу, указанному в реестре членов Партнерства, или вручается лично под роспись, а также сообщение о проведении годового Общего собрания членов Партнерства и информация (материалы), предоставляемая членам Партнерства при подготовке к проведению годового Общего собрания членов Партнерства, размещаются на сайте Партнерства http://www.izsro.ru/.

13.9. Утвердить текст Сообщения о проведении годового Общего собрания членов Партнерства (Приложение № 1).

13.10. Утвердить формы бюллетеней для голосования по вопросам повестки дня годового Общего собрания членов Партнерства (Приложение № 2).

Приложение:
Приложение № 1 – Сообщение о проведении годового Общего собрания членов Партнерства - 2 л.
Приложение № 2 – Формы бюллетеней для голосования по вопросам повестки дня годового Общего собрания членов Партнерства – 11 л.

Председатель Совета Партнерства **А.Б. Скрепнюк**

Секретарь Совета Партнерства **А.А. Дроганова**

БЮЛЛЕТЕНЬ № 1
ДЛЯ ГОЛОСОВАНИЯ ПО ВОПРОСАМ ПОВЕСТКИ ДНЯ
ГОДОВОГО ОБЩЕГО СОБРАНИЯ ЧЛЕНОВ
НП «ИНЖЕНЕР-ИЗЫСКАТЕЛЬ»

Полное фирменное наименование Партнерства:
Некоммерческое партнерство «Объединение организаций выполняющих инженерные изыскания в газовой и нефтяной отрасли «Инженер-Изыскатель»

Место нахождения НП «Инженер-Изыскатель»: 125367, г. Москва, ул. Габричевского, д.5, корп.1

Форма проведения годового Общего собрания членов Партнерства: **очная** (совместное присутствие членов для обсуждения вопросов повестки дня и принятия решений по вопросам повестки дня, поставленным на голосование).
Дата и время проведения: ***28 мая 2014 года, начало в 14 часов 00 минут.***
Место проведения: ***г. Москва, ул. Новый Арбат, д. 36/9, Здание Правительства Москвы, большой зал.***

Член Партнерства _____
(наименование)

Поставьте знак «V» справа от наименования <u>только одного</u> варианта голосования, в пользу которого сделан выбор.

Формулировка вопроса №1: **Об утверждении Отчета Совета Партнерства за 2013 год.**
Формулировка решения по вопросу №1: Утвердить Отчет Совета Партнерства за 2013 год.

«ЗА» ☐ **«ПРОТИВ»** ☐ **«ВОЗДЕРЖАЛСЯ»** ☐

Подпись представителя члена Партнерства

При отсутствии подписи члена Партнерства (уполномоченного представителя члена Партнерства) бюллетень недействителен!

БЮЛЛЕТЕНЬ № 2
ДЛЯ ГОЛОСОВАНИЯ ПО ВОПРОСАМ ПОВЕСТКИ ДНЯ
ГОДОВОГО ОБЩЕГО СОБРАНИЯ ЧЛЕНОВ
НП «ИНЖЕНЕР-ИЗЫСКАТЕЛЬ»

Полное фирменное наименование Партнерства:
Некоммерческое партнерство «Объединение организаций выполняющих инженерные изыскания в газовой и нефтяной отрасли «Инженер-Изыскатель»

Место нахождения НП «Инженер-Изыскатель»: 125367, г. Москва, ул. Габричевского, д.5, корп.1

Форма проведения годового Общего собрания членов Партнерства: **очная** (совместное присутствие членов для обсуждения вопросов повестки дня и принятия решений по вопросам повестки дня, поставленным на голосование).
Дата и время проведения: ***28 мая 2014 года, начало в 14 часов 00 минут.***
Место проведения: ***г. Москва, ул. Новый Арбат, д. 36/9, Здание Правительства Москвы, большой зал.***

Член Партнерства _____
(наименование)

Поставьте знак «V» справа от наименования <u>только одного</u> варианта голосования, в пользу которого сделан выбор.

Формулировка вопроса №2: **Об утверждении Отчета Директора о финансово-хозяйственной деятельности Партнерства в 2013 году.**
Формулировка решения по вопросу №2: Утвердить Отчет Директора о финансово-хозяйственной деятельности Партнерства в 2013 году.

«ЗА» ☐ **«ПРОТИВ»** ☐ **«ВОЗДЕРЖАЛСЯ»** ☐

Подпись представителя члена Партнерства

При отсутствии подписи члена Партнерства (уполномоченного представителя члена Партнерства) бюллетень недействителен!

БЮЛЛЕТЕНЬ № 3
ДЛЯ ГОЛОСОВАНИЯ ПО ВОПРОСАМ ПОВЕСТКИ ДНЯ
ГОДОВОГО ОБЩЕГО СОБРАНИЯ ЧЛЕНОВ
НП «ИНЖЕНЕР-ИЗЫСКАТЕЛЬ»

Полное фирменное наименование Партнерства:
Некоммерческое партнерство «Объединение организаций выполняющих инженерные изыскания в газовой и нефтяной отрасли «Инженер-Изыскатель»

Место нахождения НП «Инженер-Изыскатель»: 125367, г. Москва, ул. Габричевского, д.5, корп.1

Форма проведения годового Общего собрания членов Партнерства: **очная** (совместное присутствие членов для обсуждения вопросов повестки дня и принятия решений по вопросам повестки дня, поставленным на голосование).
Дата и время проведения: ***28 мая 2014 года, начало в 14 часов 00 минут.***
Место проведения: ***г. Москва, ул. Новый Арбат, д. 36/9, Здание Правительства Москвы, большой зал.***

Член Партнерства _____
(наименование)

Поставьте знак «V» справа от наименования <u>только одного</u> варианта голосования, в пользу которого сделан выбор.

Формулировка вопроса №3: **Об утверждении годовой бухгалтерской отчетности Партнерства за 2013 год.**
Формулировка решения по вопросу №3: Утвердить годовую бухгалтерскую отчетность Партнерства за 2013 год.

«ЗА» ☐ **«ПРОТИВ»** ☐ **«ВОЗДЕРЖАЛСЯ»** ☐

Подпись представителя члена Партнерства

При отсутствии подписи члена Партнерства (уполномоченного представителя члена Партнерства) бюллетень недействителен!

БЮЛЛЕТЕНЬ № 4
ДЛЯ ГОЛОСОВАНИЯ ПО ВОПРОСАМ ПОВЕСТКИ ДНЯ
ГОДОВОГО ОБЩЕГО СОБРАНИЯ ЧЛЕНОВ
НП «ИНЖЕНЕР-ИЗЫСКАТЕЛЬ»

Полное фирменное наименование Партнерства:
Некоммерческое партнерство «Объединение организаций выполняющих инженерные изыскания в газовой и нефтяной отрасли «Инженер-Изыскатель»

Место нахождения НП «Инженер-Изыскатель»: 125367, г. Москва, ул. Габричевского, д.5, корп.1

Форма проведения годового Общего собрания членов Партнерства: **очная** (совместное присутствие членов для обсуждения вопросов повестки дня и принятия решений по вопросам повестки дня, поставленным на голосование).
Дата и время проведения: ***28 мая 2014 года, начало в 14 часов 00 минут.***
Место проведения: ***г. Москва, ул. Новый Арбат, д. 36/9, Здание Правительства Москвы, большой зал.***

Член Партнерства _____
(наименование)

Поставьте знак «V» справа от наименования <u>только одного</u> варианта голосования, в пользу которого сделан выбор.

Формулировка вопроса №4: **Об утверждении Сметы Партнерства на 2014 год.**
Формулировка решения по вопросу №4: Утвердить Смету Партнерства на 2014 год.

«ЗА» ☐ **«ПРОТИВ»** ☐ **«ВОЗДЕРЖАЛСЯ»** ☐

Подпись представителя члена Партнерства

При отсутствии подписи члена Партнерства (уполномоченного представителя члена Партнерства) бюллетень недействителен!

БЮЛЛЕТЕНЬ № 5
ДЛЯ ГОЛОСОВАНИЯ ПО ВОПРОСАМ ПОВЕСТКИ ДНЯ
ГОДОВОГО ОБЩЕГО СОБРАНИЯ ЧЛЕНОВ
НП «ИНЖЕНЕР-ИЗЫСКАТЕЛЬ»

Полное фирменное наименование Партнерства:
Некоммерческое партнерство «Объединение организаций выполняющих инженерные изыскания в газовой и нефтяной отрасли «Инженер-Изыскатель»

Место нахождения НП «Инженер-Изыскатель»: 125367, г. Москва, ул. Габричевского, д.5, корп.1

Форма проведения годового Общего собрания членов Партнерства: **очная** (совместное присутствие членов для обсуждения вопросов повестки дня и принятия решений по вопросам повестки дня, поставленным на голосование).
Дата и время проведения: ***28 мая 2014 года, начало в 14 часов 00 минут.***
Место проведения: ***г. Москва, ул. Новый Арбат, д. 36/9, Здание Правительства Москвы, большой зал.***

Член Партнерства _____
(наименование)

Поставьте знак «V» справа от наименования <u>только одного</u> варианта голосования, в пользу которого сделан выбор.

Формулировка вопроса №5: **Об утверждении Требований к сертификации систем менеджмента качества членов Партнерства в новой редакции.**
Формулировка решения по вопросу №5: Утвердить Требования к сертификации систем менеджмента качества членов Партнерства в новой редакции.

«ЗА» ☐ **«ПРОТИВ»** ☐ **«ВОЗДЕРЖАЛСЯ»** ☐

Подпись представителя члена Партнерства

При отсутствии подписи члена Партнерства (уполномоченного представителя члена Партнерства) бюллетень недействителен!

БЮЛЛЕТЕНЬ № 6
ДЛЯ ГОЛОСОВАНИЯ ПО ВОПРОСАМ ПОВЕСТКИ ДНЯ
ГОДОВОГО ОБЩЕГО СОБРАНИЯ ЧЛЕНОВ
НП «ИНЖЕНЕР-ИЗЫСКАТЕЛЬ»

Полное фирменное наименование Партнерства:
Некоммерческое партнерство «Объединение организаций выполняющих инженерные изыскания в газовой и нефтяной отрасли «Инженер-Изыскатель»

Место нахождения НП «Инженер-Изыскатель»: 125367, г. Москва, ул. Габричевского, д.5, корп.1

Форма проведения годового Общего собрания членов Партнерства: **очная** (совместное присутствие членов для обсуждения вопросов повестки дня и принятия решений по вопросам повестки дня, поставленным на голосование).
Дата и время проведения: ***28 мая 2014 года, начало в 14 часов 00 минут.***
Место проведения: ***г. Москва, ул. Новый Арбат, д. 36/9, Здание Правительства Москвы, большой зал.***

Член Партнерства _____
(наименование)

Поставьте знак «V» справа от наименования <u>только одного</u> варианта голосования, в пользу которого сделан выбор.

Формулировка вопроса №6: **Об утверждении Положения о предоставлении информации о своей деятельности членами Партнерства в Партнерство в новой редакции.**
Формулировка решения по вопросу №6: Утвердить Положение о предоставлении информации о своей деятельности членами Партнерства в Партнерство в новой редакции.

«ЗА» ☐ **«ПРОТИВ»** ☐ **«ВОЗДЕРЖАЛСЯ»** ☐

Подпись представителя члена Партнерства

При отсутствии подписи члена Партнерства (уполномоченного представителя члена Партнерства) бюллетень недействителен!

БЮЛЛЕТЕНЬ № 7
ДЛЯ ГОЛОСОВАНИЯ ПО ВОПРОСАМ ПОВЕСТКИ ДНЯ
ГОДОВОГО ОБЩЕГО СОБРАНИЯ ЧЛЕНОВ
НП «ИНЖЕНЕР-ИЗЫСКАТЕЛЬ»

Полное фирменное наименование Партнерства:
Некоммерческое партнерство «Объединение организаций выполняющих инженерные изыскания в газовой и нефтяной отрасли «Инженер-Изыскатель»

Место нахождения НП «Инженер-Изыскатель»: 125367, г. Москва, ул. Габричевского, д.5, корп.1

Форма проведения годового Общего собрания членов Партнерства: **очная** (совместное присутствие членов для обсуждения вопросов повестки дня и принятия решений по вопросам повестки дня, поставленным на голосование).
Дата и время проведения: ***28 мая 2014 года, начало в 14 часов 00 минут.***
Место проведения: ***г. Москва, ул. Новый Арбат, д. 36/9, Здание Правительства Москвы, большой зал.***

Член Партнерства _____
(наименование)

Поставьте знак «V» справа от наименования <u>только одного</u> варианта голосования, в пользу которого сделан выбор.

Формулировка вопроса №7: **Об утверждении Правил контроля в области саморегулирования в новой редакции.**
Формулировка решения по вопросу №7: Утвердить Правила контроля в области саморегулирования в новой редакции.

«ЗА» ☐ **«ПРОТИВ»** ☐ **«ВОЗДЕРЖАЛСЯ»** ☐

Подпись представителя члена Партнерства

При отсутствии подписи члена Партнерства (уполномоченного представителя члена Партнерства) бюллетень недействителен!

БЮЛЛЕТЕНЬ № 8
ДЛЯ ГОЛОСОВАНИЯ ПО ВОПРОСАМ ПОВЕСТКИ ДНЯ
ГОДОВОГО ОБЩЕГО СОБРАНИЯ ЧЛЕНОВ
НП «ИНЖЕНЕР-ИЗЫСКАТЕЛЬ»

Полное фирменное наименование Партнерства:
Некоммерческое партнерство «Объединение организаций выполняющих инженерные изыскания в газовой и нефтяной отрасли «Инженер-Изыскатель»

Место нахождения НП «Инженер-Изыскатель»: 125367, г. Москва, ул. Габричевского, д.5, корп.1

Форма проведения годового Общего собрания членов Партнерства: **очная** (совместное присутствие членов для обсуждения вопросов повестки дня и принятия решений по вопросам повестки дня, поставленным на голосование).
Дата и время проведения: ***28 мая 2014 года, начало в 14 часов 00 минут.***
Место проведения: ***г. Москва, ул. Новый Арбат, д. 36/9, Здание Правительства Москвы, большой зал.***

Член Партнерства _____
(наименование)

Поставьте знак «V» справа от наименования <u>только одного</u> варианта голосования, в пользу которого сделан выбор.

Формулировка вопроса №8: **О выплате вознаграждений членам Ревизионной комиссии Партнерства по итогам работы в 2013 году.**
Формулировка решения по вопросу №8: Выплатить вознаграждение членам Ревизионной комиссии Партнерства по итогам работы в 2013 году в следующем размере: 1. Фомина Людмила Павловна – 80 000 (восемьдесят тысяч) рублей 00 копеек. 2. Полякова Ольга Владимировна – 40 000 (сорок тысяч) рублей 00 копеек. 3. Лабецкая Любовь Федоровна – 40 000 (сорок тысяч) рублей 00 копеек.

«ЗА» ☐ **«ПРОТИВ»** ☐ **«ВОЗДЕРЖАЛСЯ»** ☐

Подпись представителя члена Партнерства

При отсутствии подписи члена Партнерства (уполномоченного представителя члена Партнерства) бюллетень недействителен!

БЮЛЛЕТЕНЬ № 9
ДЛЯ ГОЛОСОВАНИЯ ПО ВОПРОСАМ ПОВЕСТКИ ДНЯ
ГОДОВОГО ОБЩЕГО СОБРАНИЯ ЧЛЕНОВ
НП «ИНЖЕНЕР-ИЗЫСКАТЕЛЬ»

Полное фирменное наименование Партнерства:
Некоммерческое партнерство «Объединение организаций выполняющих инженерные в газовой и нефтяной отрасли «Инженер-Изыскатель»

Место нахождения НП «Инженер-Изыскатель»: 125367, г. Москва, ул. Габричевского, д.5, корп.1

Форма проведения годового Общего собрания членов Партнерства: **очная** (совместное присутствие членов для обсуждения вопросов повестки дня и принятия решений по вопросам повестки дня, поставленным на голосование).
Дата и время проведения: ***28 мая 2014 года, начало в 14 часов 00 минут.***
Место проведения: ***г. Москва, ул. Новый Арбат, д. 36/9, Здание Правительства Москвы, большой зал.***

Поставьте знак «V» справа от наименования <u>только одного</u> варианта голосования, в пользу которого сделан выбор.

Формулировка вопроса №9: **Об избрании Ревизионной комиссии Партнерства.**
Формулировка решения по вопросу №9: Избрать Ревизионную комиссию Партнерства в составе 3 человек сроком на 2 года в следующем составе: 1. Фомина Людмила Павловна; 2. Полякова Ольга Владимировна; 3. Сальков Николай Петрович.

«ЗА» ☐ **«ПРОТИВ»** ☐ **«ВОЗДЕРЖАЛСЯ»** ☐

Голосование по вопросу №9 повестки дня является тайным

БЮЛЛЕТЕНЬ № 10
ДЛЯ ГОЛОСОВАНИЯ ПО ВОПРОСАМ ПОВЕСТКИ ДНЯ
ГОДОВОГО ОБЩЕГО СОБРАНИЯ ЧЛЕНОВ
НП «ИНЖЕНЕР-ИЗЫСКАТЕЛЬ»

Полное фирменное наименование Партнерства:
Некоммерческое партнерство «Объединение организаций выполняющих инженерные изыскания в газовой и нефтяной отрасли «Инженер-Изыскатель»

Место нахождения НП «Инженер-Изыскатель»: 125367, г. Москва, ул. Габричевского, д.5, корп.1

Форма проведения годового Общего собрания членов Партнерства: **очная** (совместное присутствие членов для обсуждения вопросов повестки дня и принятия решений по вопросам повестки дня, поставленным на голосование).
Дата и время проведения: ***28 мая 2014 года, начало в 14 часов 00 минут.***
Место проведения: ***г. Москва, ул. Новый Арбат, д. 36/9, Здание Правительства Москвы, большой зал.***

Поставьте знак «V» справа от наименования <u>только одного</u> варианта голосования, в пользу которого сделан выбор.

Формулировка вопроса №10: **О внесении изменений в состав Совета Партнерства.**
Формулировка решения по вопросу №10: 10.1. Досрочно прекратить полномочия Гафарова Наиля Анатольевича в качестве члена Совета Партнерства. 10.2. Избрать Минликаева Валерия Зиряковича в Совет Партнерства. 10.3. Определить срок полномочий Минликаева Валерия Зиряковича в качестве члена Совета Партнерства до момента прекращения срока полномочий ранее избранного состава Совета Партнерства (Протокол Общего собрания членов Партнерства № 9 от 11.10.2012 г.).

«ЗА» ☐ **«ПРОТИВ»** ☐ **«ВОЗДЕРЖАЛСЯ»** ☐

Голосование по вопросу №10 повестки дня является тайным

Данный бюллетень заполняется и сдается после оглашения результатов голосования по вопросу повестки дня № 10 «О внесении изменений в состав Совета Партнерства»!

БЮЛЛЕТЕНЬ № 11
ДЛЯ ГОЛОСОВАНИЯ ПО ВОПРОСАМ ПОВЕСТКИ ДНЯ
ГОДОВОГО ОБЩЕГО СОБРАНИЯ ЧЛЕНОВ
НП «ИНЖЕНЕР-ИЗЫСКАТЕЛЬ»

Полное фирменное наименование Партнерства:
Некоммерческое партнерство «Объединение организаций выполняющих инженерные изыскания в газовой и нефтяной отрасли «Инженер-Изыскатель»

Место нахождения НП «Инженер-Изыскатель»: 125367, г. Москва, ул. Габричевского, д.5, корп.1

Форма проведения внеочередного Общего собрания членов Партнерства: **очная** (совместное присутствие членов для обсуждения вопросов повестки дня и принятия решений по вопросам повестки дня, поставленным на голосование).
Дата и время проведения: ***28 мая 2014 года, начало в 14 часов 00 минут.***
Место проведения: ***г. Москва, ул. Новый Арбат, д. 36/9, Здание Правительства Москвы, большой зал.***

Поставьте знак «V» справа от наименования только одного варианта голосования, в пользу которого сделан выбор.

Формулировка вопроса №11: **Об избрании Председателя Совета Партнерства.**		
Формулировка решения по вопросу №11: Избрать Председателем Совета Партнерства с 27.11.2014 г. сроком на 2 года в соответствии с п. 9.13 Устава Партнерства члена Совета Партнерства:		
1. Скрепнюк Андрей Борисович	**«ЗА»**	
2. Прозоров Сергей Фролович	**«ЗА»**	
3. Алимов Сергея Викторовича	**«ЗА»**	
4. Небабин Владимир Викторович	**«ЗА»**	
5. Минликаев Валерий Зирякович	**«ЗА»**	
6. Шеховцов Андрея Викторович	**«ЗА»**	
7. Разумов Дмитрий Валерьевич	**«ЗА»**	
8. Милованов Виктор Иванович	**«ЗА»**	
9. Савченков Сергей Викторович	**«ЗА»**	
10. Цыбульский Павел Геннадьевич	**«ЗА»**	
11. Азарх Михаил Михайлович	**«ЗА»**	

Голосование по вопросу №11 повестки дня является тайным

Информационно-
аналитический отдел

_____№_____

УТВЕРЖДАЮ
Директор
НП «Инженер-Изыскатель»

_____М.М. Азарх

«___»_____2014г.

КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПАРТНЕРСТВА

г. Москва

Оглавление

1. Определения

Настоящей Концепцией обеспечения безопасности сведений, представляемых членами Партнерства (далее - Концепция) предусмотрены следующие термины и их определения:

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации ее деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационную систему) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть

раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

Информационная система (ИС) – совокупность конфиденциальных сведений, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких сведений с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность информации – обязательное для соблюдения оператором или иным получившим доступ к конфиденциальным сведениям лицом, требование не допускать их распространение без согласия обладателя информации или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему и (или) выходящей из информационной системы.

Нарушитель безопасности конфиденциальных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности конфиденциальных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Партнерство – некоммерческое партнерство «Объединение организаций выполняющих инженерные изыскания в газовой и нефтяной отрасли «Инженер-Изыскатель».

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы – лицо, участвующее в функционировании информационной системы или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Распространение конфиденциальных сведений – действия, направленные на передачу конфиденциальных сведений определенному кругу лиц (передача конфиденциальной информации) или на ознакомление с конфиденциальными сведениями неограниченного круга лиц, в том числе обнародование конфиденциальных сведений в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к конфиденциальным сведениям каким-либо иным способом.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Технические средства информационной системы – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки конфиденциальной информации (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Угроза безопасности конфиденциальных сведений – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к конфиденциальным сведениям, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации, а также иных несанкционированных действий при их обработке в информационной системе.

Уничтожение конфиденциальных сведений – действия, в результате которых невозможно восстановить содержание конфиденциальных сведений в информационной системе или в результате которых уничтожаются материальные носители конфиденциальной информации.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой

информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2. Обозначения и сокращения

АВС – антивирусные средства
АРМ – автоматизированное рабочее место
ВТСС – вспомогательные технические средства и системы
ИС – информационная система
КЗ – контролируемая зона
КИ – конфиденциальная информация
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
НСД – несанкционированный доступ
ОС – операционная система
ПДн – персональные данные
ПМВ – программно-математическое воздействие
ПО – программное обеспечение
ПЭМИН – побочные электромагнитные излучения и наводки
САЗ – система анализа защищенности
СЗИ – средства защиты информации
СЗКИ – система (подсистема) защиты конфиденциальной информации
СОВ – система обнаружения вторжений
ТКУИ – технические каналы утечки информации

3. Введение

Настоящая Концепция является официальным документом, в котором определена система взглядов на обеспечение безопасности конфиденциальной информации, в состав которой входят сведения, предоставляемые членами Партнерства, обрабатываемой в ИС Партнерства.

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты конфиденциальной информации Партнерства и его членов. Концепция определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

Концепция разработана в соответствии с системным подходом к обеспечению информационной безопасности. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты КИ, с позиции комплексного применения технических и организационных мер и средств защиты.

Под информационной безопасностью КИ понимается защищенность конфиденциальной информации и обрабатывающей ее инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности КИ, а также к прогнозированию и предотвращению таких воздействий.

Концепция служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности Партнерства, а также нормативных и методических документов, обеспечивающих ее реализацию, и не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и защиту информации.

Концепция является методологической основой для:

- формирования и проведения единой политики в области обеспечения безопасности КИ, в том числе сведений, представляемых членами Партнерства;
- принятия управленческих решений и разработки практических мер по воплощению политики безопасности КИ и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз КИ;
- координации деятельности структурных подразделений Партнерства при проведении работ по развитию и эксплуатации информационных систем с соблюдением требований обеспечения безопасности КИ;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности КИ в ИС Партнерства.

Область применения Концепции распространяется на все подразделения Партнерства, эксплуатирующие, обслуживающие технические и программные средства ИС, в которых осуществляется автоматизированная обработка КИ, в том числе сведений, представляемых членами Партнерства.

Правовой базой для разработки настоящей Концепции служат требования действующих в России законодательных и нормативных документов по обеспечению безопасности информации.

4. Общие положения

Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты конфиденциальной информации (СЗКИ) Партнерства. Концепция определяет основные требования и базовые подходы к их реализации для достижения требуемого уровня безопасности информации.

СЗКИ представляет собой совокупность организационных и технических мероприятий для защиты КИ от неправомерного или случайного доступа к ней, уничтожения, изменения, блокирования, копирования, распространения КИ, а также иных неправомерных действий с ней.

Безопасность КИ достигается путем исключения несанкционированного, в том числе случайного, доступа к КИ, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение КИ, а также иных несанкционированных действий.

Структура, состав и основные функции СЗКИ определяются исходя из класса ИС. СЗКИ включает организационные меры и технические средства защиты информации (в том числе шифровальные, криптографические), средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки КИ, а также используемые в информационной системе информационные технологии.

Эти меры призваны обеспечить:

- конфиденциальность информации (защита от несанкционированного ознакомления);
- целостность информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- доступность информации (возможность за приемлемое время получить требуемую информационную услугу).

Стадии создания СЗКИ включают:

- предпроектная стадия, включающая предпроектное обследование ИС, разработку технического (частного технического) задания на ее создание;
- стадия проектирования и реализации ИС, включающая разработку СЗКИ в составе ИС;
- стадия ввода в действие СЗКИ, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия ИС требованиям безопасности информации.

Организационные меры предусматривают создание и поддержание правовой базы безопасности КИ и разработку (введение в действие) предусмотренных Политикой информационной безопасности ИС следующих организационно-распорядительных документов:

- План мероприятий по обеспечению защиты КИ при ее обработке в ИС;
- Правила по контролю за режимом коммерческой тайны;

- Инструкция администратора информационной системы обработки сведений, представляемых членами Партнерства;
- Инструкция пользователя компьютерной локально вычислительной сетью Партнерства;
- Перечень конфиденциальной информации Партнерства;
- Рекомендации по ограничению использования интернет ресурсов на АРМ, обрабатывающих КИ.

Технические меры защиты реализуются при помощи соответствующих программно-технических средств и методов защиты.

Перечень необходимых мер защиты информации определяется по результатам внутренней проверки безопасности ИС Партнерства.

5. Задачи Системы защиты конфиденциальной информации

Основной целью СЗКИ является минимизация ущерба от возможной реализации угроз безопасности КИ.

Для достижения основной цели система безопасности КИ должна обеспечивать эффективное решение следующих задач:

- защиту от вмешательства в процесс функционирования ИС посторонних лиц (возможность использования автоматизированной системы и доступ к ее ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);
- разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИС (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИС для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:

а) к информации, циркулирующей в ИС;

б) средствам вычислительной техники ИС;

в) аппаратным, программным и криптографическим средствам защиты, используемым в ИС;

- регистрацию действий пользователей при использовании защищаемых ресурсов ИС в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;
- контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;
- защиту от несанкционированной модификации и контроль целостности используемых в ИС программных средств, а также защиту системы от внедрения несанкционированных программ;
- защиту КИ от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;
- защиту КИ, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;
- обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;

- своевременное выявление источников угроз безопасности КИ, причин и условий, способствующих нанесению ущерба субъектам КИ, создание механизма оперативного реагирования на угрозы безопасности КИ и негативные тенденции;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности КИ.

6. Перечень информационных систем

В Партнерстве производится обработка конфиденциальной информации (КИ) в информационных системах (ИС).

Перечень ИС определяется на основании Отчета по результатам внутренней проверки информационных ресурсов Партнерства.

7. Перечень объектов защиты

Объектами защиты являются – информация, обрабатываемая в ИС, и технические средства ее обработки и защиты. Перечень конфиденциальной информации, подлежащей защите, определен в Перечне конфиденциальной информации Партнерства.

Объекты защиты включают:

1) Обрабатываемая информация.
2) Технологическая информация.
3) Программно-технические средства обработки.
4) Средства защиты КИ.
5) Каналы информационного обмена и телекоммуникации.
6) Объекты и помещения, в которых размещены компоненты ИС.

8. Классификация пользователей ИС

Пользователем ИС является лицо, участвующее в функционировании информационной системы или использующее результаты ее функционирования. Пользователями ИС являются сотрудники Партнерства, имеющие доступ к ИС и ее ресурсам в соответствии с установленным в НП порядком, и в соответствии со своими функциональными обязанностями.

Пользователи ИС делятся на три основные категории:

1. Администратор ИС. Сотрудники Партнерства, которые занимаются настройкой, внедрением и сопровождением системы. Администратор ИС обладает следующим уровнем доступа:
   - обладает полной информацией о системном и прикладном программном обеспечении ИС;

- обладает полной информацией о технических средствах и конфигурации ИС;
- имеет доступ ко всем техническим средствам обработки информации и данным ИС;
- обладает правами конфигурирования и административной настройки технических средств ИС.

2. Программист-разработчик ИС. Сотрудники Партнерства или сторонних организаций, которые занимаются разработкой программного обеспечения. Разработчик ИС обладает следующим уровнем доступа:
- обладает информацией об алгоритмах и программах обработки информации на ИС;
- обладает возможностями устранения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИС на стадии ее разработки, внедрения и сопровождения;
- может располагать любыми фрагментами информации о топологии ИС и технических средствах обработки и защиты КИ, обрабатываемой в ИС.

3. Оператор ИС. Сотрудники подразделений Партнерства участвующие в процессе эксплуатации ИС. Оператор ИС обладает следующим уровнем доступа:
- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству КИ;
- располагает конфиденциальными данными, к которым имеет доступ.

Категории пользователей должны быть определены для каждой ИС. Должно быть уточнено разделение сотрудников внутри категорий, в соответствии с типами пользователей, определенными в Политике информационной безопасности.

Все выявленные группы пользователей отражаются в Отчете по результатам внутренней проверки. На основании Отчета определяются права доступа к элементам ИС для всех групп.

9. Основные принципы построения системы комплексной защиты информации

Построение системы обеспечения безопасности КИ Партнерства и ее функционирование должны осуществляться в соответствии со следующими основными принципами:
- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- персональная ответственность;
- минимизация полномочий;

- взаимодействие и сотрудничество;
- гибкость системы защиты;
- открытость алгоритмов и механизмов защиты;
- простота применения средств защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- обязательность контроля.

Законность

Предполагает осуществление защитных мероприятий и разработку СЗКИ Партнерства в соответствии с действующим законодательством в области защиты КИ и других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции.

Пользователи и обслуживающий персонал ИС Партнерства должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за защиту КИ.

Системность

Системный подход к построению СЗКИ Партнерства предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности КИ Партнерства.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки КИ, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

Комплексность

Комплексное использование методов и средств защиты предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

Защита должна быть многоуровневой. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболее укрепленных рубежей призваны быть средства криптографической защиты, реализованные с использованием технологии VPN (персональная защищенная сеть). Прикладной уровень защиты (комплекс программно-аппаратных средств, регистрирующих и сравнивающих события, происходящие в ИС, с эталонным списком разрешенных событий и предотвращающий несанкционированные процессы), учитывающий особенности предметной области (комплекс информации, входящий в предмет обработки ИС, образующей эталон для прикладного уровня защиты), представляет внутренний рубеж защиты.

Непрерывность

ИС должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода ИС в незащищенное состояние.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных закладок и других средств преодоления системы защиты после восстановления ее функционирования.

Своевременность

Предполагает упреждающий характер мер обеспечения безопасности КИ, т.е. постановку задач по комплексной защите ИС и реализацию мер обеспечения безопасности КИ на ранних стадиях разработки ИС в целом и ее системы защиты информации, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

Преемственность и непрерывность совершенствования

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИС и ее системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности КИ и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

Минимизация полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено».

Доступ к КИ должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность ИС Партнерства, для снижения вероятности возникновения негативных действий, связанных с человеческим фактором.

В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности специалисту по защите информации.

Гибкость системы защиты

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Однако это не означает, что информация о конкретной системе защиты должна быть общедоступна.

Простота применения средств защиты

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных в установленном порядке пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

Должна достигаться автоматизация максимального числа действий пользователей и администраторов ИС.

Научная обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности КИ.

СЗКИ должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности КИ, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами по защите информации Партнерства.

Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности КИ на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

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.

10. Меры, методы и средства обеспечения требуемого уровня защищенности

Обеспечение требуемого уровня защищенности должно достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности ИС подразделяются на:

- законодательные (правовые);
- морально-этические;
- организационные (административные);
- физические;
- технические (аппаратные и программные).

Перечень выбранных мер обеспечения безопасности отражается в Плане мероприятий по обеспечению защиты персональных данных.

Законодательные (правовые) меры защиты

К правовым мерам защиты относятся действующие в стране законы и иные нормативные акты, регламентирующие правила обращения с КИ, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию КИ и являющиеся сдерживающим фактором для потенциальных нарушителей.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения ЭВМ в стране или обществе. Несоблюдение этих норм ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний.

Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений. Морально-этические меры защиты снижают вероятность возникновения негативных действий связанных с человеческим фактором.

Организационные (административные) меры защиты

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования ИС, использование ресурсов ИС, деятельность

обслуживающего персонала, а также порядок взаимодействия пользователей с ИС таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

Главная цель административных мер, предпринимаемых на высшем управленческом уровне, – сформировать Политику информационной безопасности КИ (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Реализация Политики информационной безопасности КИ в ИС состоит из мер административного уровня и организационных (процедурных) мер защиты информации.

К административному уровню относятся решения руководства, затрагивающие деятельность ИС в целом. Примером таких решений могут быть:

- принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности КИ, определение ответственных за ее реализацию;
- формулирование целей, постановка задач, определение направлений деятельности в области безопасности КИ;
- принятие решений по вопросам реализации программы безопасности, которые рассматриваются на уровне Партнерства в целом;
- обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности КИ, определить, какими ресурсами (материальные, трудовые) они будут достигнуты, и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью ИС.

На организационном уровне определяются процедуры и правила достижения целей и решения задач Политики информационной безопасности КИ. Эти правила определяют:

- какова область применения политики безопасности КИ;
- каковы роли и обязанности должностных лиц, отвечающих за проведение политики безопасности КИ, а также их ответственность;
- кто имеет права доступа к КИ;
- какими мерами и средствами обеспечивается защита КИ;
- какими мерами и средствами обеспечивается контроль за соблюдением введенного режима безопасности.

Организационные меры должны:

- предусматривать регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;
- определять коалиционные и иерархические принципы и методы разграничения доступа к КИ;

- определять порядок работы с программно-математическими и техническими (аппаратными) средствами защиты и криптозащиты и других защитных механизмов;
- сформулировать процедуру противодействия НСД пользователями на этапах аутентификации, авторизации, идентификации, обеспечивающую гарантии реализации прав и ответственности субъектов информационных отношений.

Организационные меры должны состоять из:
- регламента доступа в помещения ИС;
- порядка допуска сотрудников к использованию ресурсов ИС Партнерства;
- регламента процессов ведения баз данных и осуществления модификации информационных ресурсов;
- регламента процессов обслуживания и осуществления модификации аппаратных и программных ресурсов ИС;
- инструкций пользователей ИС (администратора ИС, администратора безопасности, оператора ИС);
- инструкции пользователя при возникновении внештатных ситуаций.

Физические меры защиты

Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

Технические меры защиты

Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИС и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

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

- средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей ИС;
- средства разграничения доступа зарегистрированных пользователей системы к ресурсам ИС Партнерства;
- средства обеспечения и контроля целостности программных и информационных ресурсов;
- средства оперативного контроля и регистрации событий безопасности;
- криптографические средства защиты КИ.

На технические средства защиты от НСД возлагается решение следующих основных задач (в соответствии с Руководящими документами ФСТЭК России и ГОСТ):

- идентификация и аутентификации пользователей при помощи имен и/или специальных аппаратных средств (Touch Memory, Smart Card и т.п.);
- 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;
- регистрация всех действий пользователя в защищенном журнале, наличие нескольких уровней регистрации;
- централизованный сбор, хранение и обработка на файловом сервере и внешнем носителе 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 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.

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

- обеспечена физическая целостность всех компонентов ИС;
- каждый сотрудник (пользователь ИС) или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения

им своих функциональных обязанностей полномочия по доступу к ресурсам системы;

- в ИС Партнерства разработка и отладка программ осуществляется за пределами ИС, на испытательных стендах;
- все изменения конфигурации технических и программных средств ИС производятся в строго установленном порядке (регистрируются и контролируются) только на основании распоряжений руководства Партнерства;
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.);
- специалистами Партнерства осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

Средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей

В целях предотвращения работы с ИС посторонних лиц необходимо обеспечить возможность распознавания системой каждого законного пользователя (или ограниченных групп пользователей). Для этого в системе (в защищенном месте) должен храниться 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 обязан себя идентифицировать, т.е. указать идентификатор, присвоенный ему в системе. Кроме того, для идентификации могут применяться различного рода устройства: магнитные карточки, ключевые вставки и т.п.

Аутентификация (подтверждение подлинности) пользователей должна осуществляться на основе использования паролей (секретных слов) или проверки уникальных характеристик (параметров) пользователей при помощи специальных биометрических средств.

Средства разграничения доступа зарегистрированных пользователей системы к ресурсам ИС

После распознавания пользователя система должна осуществлять авторизацию пользователя, то есть определять, какие права предоставлены пользователю: 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:

- 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.

Зоны ответственности и задачи конкретных технических средств защиты устанавливаются исходя из их возможностей и эксплуатационных характеристик, описанных в документации на данные средства.

Технические средства разграничения доступа должны быть составной частью единой системы контроля доступа:

- на контролируемую территорию;
- в отдельные помещения;
- к элементам ИС и элементам системы защиты информации (физический доступ);
- к информационным хранилищам (носителям информации, томам, файлам, архивам, справкам, записям и т.д.);
- к активным ресурсам (прикладным программам, задачам и т.п.).

Средства обеспечения и контроля целостности программных и информационных ресурсов

Контроль целостности программ, обрабатываемой информации и средств защиты, с целью обеспечения неизменности программной среды, определяемой предусмотренной технологией обработки, и защиты от несанкционированной корректировки информации должен обеспечиваться:

- средствами электронной цифровой подписи;
- средствами сравнения критичных ресурсов с их эталонными копиями (и восстановления в случае нарушения целостности);
- средствами разграничения доступа (запрет доступа с правами модификации или удаления).

В целях защиты информации и программ от несанкционированного уничтожения или искажения необходимо обеспечить:

- дублирование системных таблиц и данных;
- дуплексирование и зеркальное отображение данных на дисках;
- отслеживание транзакций;
- периодический контроль целостности операционной системы и пользовательских программ, а также файлов пользователей;
- антивирусный контроль;
- резервное копирование данных по заранее установленной схеме;
- хранение резервных копий вне помещения файл-сервера;
- обеспечение непрерывности электропитания для файл-серверов и критичных рабочих станций и кондиционирование электропитания для остальных станций сети.

Средства оперативного контроля и регистрации событий безопасности

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

- ведения и анализа журналов регистрации событий безопасности (системных журналов). Журналы регистрации должны вестись для каждой рабочей станции сети;
- оперативного ознакомления администратора безопасности с содержимым системного журнала любой станции и с журналом оперативных сообщений об НСД;
- получения твердой копии (печати) системного журнала;
- упорядочения системных журналов по дням и месяцам, а также установления ограничений на срок их хранения;

оперативного оповещения администратора безопасности о нарушениях.

При регистрации событий безопасности в системном журнале должна фиксироваться 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;
- вход пользователя в сеть;
- неудачная попытка входа в систему или сеть (неправильный ввод пароля);
- подключение к файловому серверу;
- запуск программы;
- завершение программы;
- оставление программы резидентно в памяти;
- попытка открытия файла недоступного для чтения;
- попытка открытия на запись файла недоступного для записи;
- попытка удаления файла недоступного для модификации;
- попытка изменения атрибутов файла недоступного для модификации;
- попытка запуска программы, недоступной для запуска;
- попытка получения доступа к недоступному каталогу;
- попытка чтения/записи информации с диска, недоступного пользователю;
- попытка запуска программы с диска, недоступного пользователю;
- нарушение целостности программ и данных системы защиты

и др.

Должны поддерживаться следующие основные способы реагирования на обнаруженные факты НСД (возможно с участием администратора безопасности):

- извещение владельца информации о НСД к его данным;
- снятие программы (задания) с дальнейшего выполнения;
- извещение администратора баз данных и администратора безопасности;
- отключение терминала (рабочей станции), с которого были осуществлены попытки НСД к информации;
- исключение нарушителя из списка зарегистрированных пользователей; подача сигнала тревоги и др.

Криптографические средства защиты информации

Одним из важнейших элементов системы обеспечения безопасности информации ИС должно быть использование криптографических методов и средств защиты информации от несанкционированного доступа при ее передаче по каналам связи.

Все средства криптографической защиты информации в ИС Партнерства должны строиться на основе базисного криптографического ядра, прошедшего всесторонние исследования специализированными организациями ФСБ России и ФСТЭК. Используемые средства криптографической защиты секретной информации должны быть сертифицированы, а вся подсистема, в которой они используются, должна быть аттестована ФСБ России и ФСТЭК. На использование криптографических средств Партнерство должно иметь лицензию ФСБ России и сертификат ФСТЭК.

Ключевая система применяемых в ИС Партнерства шифровальных средств должна обеспечивать криптографическую живучесть и многоуровневую защиту от компрометации ключевой информации, разделение пользователей по уровням обеспечения защиты и зонам их взаимодействия между собой и пользователями других уровней.

Конфиденциальность и имитозащита информации при ее передаче по каналам связи должна обеспечиваться за счет применения в системе шифросредств абонентского и на отдельных направлениях канального шифрования. Сочетание абонентского и канального шифрования информации должно обеспечивать ее сквозную защиту по всему тракту прохождения, защищать информацию в случае ее ошибочной переадресации за счет сбоев и неисправностей аппаратно-программных средств центров коммутации.

В ИС Партнерства, являющейся системой с распределенными информационными ресурсами, также должны использоваться средства формирования и проверки электронной цифровой подписи, обеспечивающие целостность и юридически доказательное подтверждение подлинности сообщений, а также аутентификацию пользователей, абонентских пунктов и подтверждение времени отправления сообщений. При этом должны

использоваться только стандартизованные алгоритмы цифровой подписи, а соответствующие средства, реализующие эти алгоритмы, должны быть сертифицированы ФСБ России и ФСТЭК.

11.Контроль эффективности системы защиты ИС Партнерства

Контроль эффективности СЗКИ должен осуществляется на периодической основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы СЗКИ (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а также прогнозирование и превентивное реагирование на новые угрозы безопасности КИ.

Контроль может проводиться как администраторами безопасности ИС (оперативный контроль в процессе информационного взаимодействия в ИС), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию (ФСТЭК России и ФСБ России) в пределах их компетенции.

Контроль может осуществляться специалистом по защите информации как с помощью штатных средств системы защиты КИ, так и с помощью специальных программных средств контроля.

Оценка эффективности мер защиты КИ проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

12.Сферы ответственности за безопасность КИ

Ответственным за разработку мер и контроль над обеспечением безопасности персональных данных является директор Партнерства. Директор может делегировать часть полномочий по обеспечению безопасности персональных данных иным сотрудникам Партнерства.

Сфера ответственности директора включает следующие направления обеспечения безопасности КИ:

- планирование и реализация мер по обеспечению безопасности КИ;
- анализ угроз безопасности КИ;
- разработку, внедрение, контроль исполнения и поддержание в актуальном состоянии политики, руководств, концепций, процедур, регламентов, инструкций и других организационных документов по обеспечению безопасности;
- контроль защищенности информационной инфраструктуры Партнерства от угроз;
- обучение и информирование пользователей ИС о порядке работы с КИ и средствами защиты;
- предотвращение, выявление, реагирование и расследование нарушений безопасности КИ.

При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к объектам защиты, с этими организациями должно быть заключено «Соглашение о конфиденциальности», либо «Соглашение о соблюдении режима безопасности КИ при выполнении работ в ИС». Подготовка типовых вариантов этих соглашений осуществляется специалистом по защите информации.

13.Модель нарушителя безопасности

Под нарушителем в Партнерстве понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты.

Нарушители подразделяются по признаку принадлежности к ИС. Все нарушители делятся на две группы:

- внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИС;
- внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИС.

14.Модель угроз безопасности

Для ИС Партнерства выделяются следующие основные категории угроз безопасности конфиденциальных сведений:

1) Угрозы от утечки по техническим каналам.
2) Угрозы несанкционированного доступа к информации.
3) Угрозы уничтожения, хищения аппаратных средств ИС, носителей информации путем физического доступа к элементам ИС.
4) Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий).
5) Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИС и СЗКИ в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.
6) Угрозы преднамеренных действий внутренних нарушителей.
7) Угрозы несанкционированного доступа по каналам связи.

15.Механизм реализации Концепции

Реализация Концепции должна осуществляться на основе перспективных программ и планов, которые составляются на основании и во исполнение:

- федеральных законов в области обеспечения информационной безопасности и защиты информации;
- указов Президента;
- постановлений Правительства Российской Федерации;
- руководящих, организационно-распорядительных и методических документов ФСТЭК России;
- потребностей ИС в средствах обеспечения безопасности информации.

16.Ожидаемый эффект от реализации Концепции

Реализация Концепции позволит:

-оценить состояние безопасности информации в ИС, выявить источники внутренних и внешних угроз информационной безопасности;

-определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;

-разработать распорядительные и нормативно-методические документы применительно к ИС;

-провести классификацию и сертификацию ИС;

-провести организационно-режимные и технические мероприятия по обеспечению безопасности КИ в ИС;

-обеспечить необходимый уровень безопасности объектов защиты.

Осуществление этих мероприятий обеспечит создание единой, целостной и скоординированной системы информационной безопасности ИС и создаст условия для ее дальнейшего совершенствования.

Специалист
по защите информации Р.В. Педанов
«___» апреля 2014 г.

СОГЛАСОВАНО

Начальник ИАО Д.Ю. Дрыгин
«___» апреля 2014 г.

Приложение №1

Лист ознакомления

Должность	Ф.И.О.	Подпись, дата

Должность	Ф.И.О.	Подпись, дата

Приложение №2

Лист регистрации изменений

№ изменения	Номера листов (страниц)				Всего листов (страниц) в докум.	Входящий номер сопроводи-тельного документа и дата	Дата
	измененных	замененных	новых	аннулированных			