

Государственное учреждения «Новгородский информационно-аналитический центр»

УТВЕРЖДАЮ

Директор Государственного
учреждения «Новгородский
информационно-аналитический центр»



В.А. Федоров

2018 г.

Регламент подключения внешних пользователей к информационной системе «Программа для ЭВМ «Региональный портал электронных услуг» Государственного учреждения «Новгородский информационно-аналитический центр»

Содержание

СОДЕРЖАНИЕ	1
ПРИНЯТЫЕ СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ	2
НОРМАТИВНО-ПРАВОВЫЕ ССЫЛКИ	3
ВВЕДЕНИЕ	4
1. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПОДКЛЮЧЕНИИ ВНЕШНИХ ПОЛЬЗОВАТЕЛЕЙ К ПОРТАЛУ	5
2. ПОРЯДОК ПОДКЛЮЧЕНИЯ ВНЕШНИХ ПОЛЬЗОВАТЕЛЕЙ К ЗАЩИЩЕННОЙ СЕТИ ПОРТАЛА	8

Принятые сокращения и определения

АРМ	- автоматизированное рабочее место;
Портал	- информационная система «Программа для ЭВМ «Региональный портал электронных услуг» (ИС);
Внешние пользователи	- внешние пользователи информационной системы «Программа для ЭВМ «Региональный портал электронных услуг» (Органы власти, Органы местного самоуправления, многофункциональные центры);
ПКИ	- парольно-ключевая информация;
Оператор	- Государственное учреждение «Новгородский информационно-аналитический центр»;
Регламент	- регламент подключения внешних пользователей к информационной системе «Программа для ЭВМ «Региональный портал электронных услуг» Государственного учреждения «Новгородский информационно-аналитический центр».

Нормативно-правовые ссылки

Настоящий документ разработан в соответствии со следующими нормативно-правовыми актами Российской Федерации (далее – НПА):

- [1] Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- [2] Приказ ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Введение

Настоящий документ разработан в соответствии с НПА [1]-[2] и регламентирует порядок подключения внешних пользователей к защищенной сети Портала, а также определяет обязательные технические и организационные требования по обеспечению информационной безопасности при подключении внешних пользователей к Порталу.

1. Требования по обеспечению информационной безопасности при подключении внешних пользователей к Порталу

1.1 Общие положения

В соответствии с НПА [1]-[2], информационное взаимодействие внешних пользователей с Оператором должно осуществляться по защищенному каналу связи.

В целях реализации требований вышеуказанных НПА, подключение к Порталу производится с использованием сертифицированных средств защиты информации, обеспечивающих безопасное информационное взаимодействие внешних пользователей с Оператором.

1.2 Основные требования

Для реализации защищенного взаимодействия внешних пользователей с Оператором на АРМ внешних пользователей, подключающихся к Порталу, должны быть выполнены следующие требования:

- обеспечение безопасного межсетевого взаимодействия;
- обеспечение защиты конфиденциальности и целостности передаваемой по каналам связи информации;
- выполнение обязательных организационных мероприятий, необходимых при эксплуатации средств криптографической защиты информации в соответствии с требованиями нормативных документов ФСБ России.

Реализация вышеуказанных требований достигается путем выполнения следующих технических и организационных мер по защите информации:

- установка и настройка на АРМ внешних пользователей сертифицированного ФСБ России средства криптографической защиты информации (программный комплекс «ViPNet Client 4.x»);
- установка и настройка на АРМ внешних пользователей сертифицированного ФСТЭК России средства антивирусной защиты информации;
- разработка необходимой документации по эксплуатации криптографических средств в соответствии с требованиями нормативных документов ФСБ России:

- Приказ «Об утверждении перечня мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты», который включает в себя следующие мероприятия:

- назначение ответственного пользователя криптосредств;
- утверждение инструкции ответственного пользователя криптосредств;

- утверждение перечня сотрудников, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности информации;
- утверждение инструкции пользователей криптосредств;
- утверждение перечня помещений, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств;
- утверждение перечня лиц, имеющих доступ в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств;
- утверждение порядка доступа в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств.
- утверждение формы журнала поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов;
- утверждение формы лицевого счета пользователя криптосредств.

Обобщенная схема информационного взаимодействия АРМ внешних пользователей с Порталом представлена на рисунке 1.

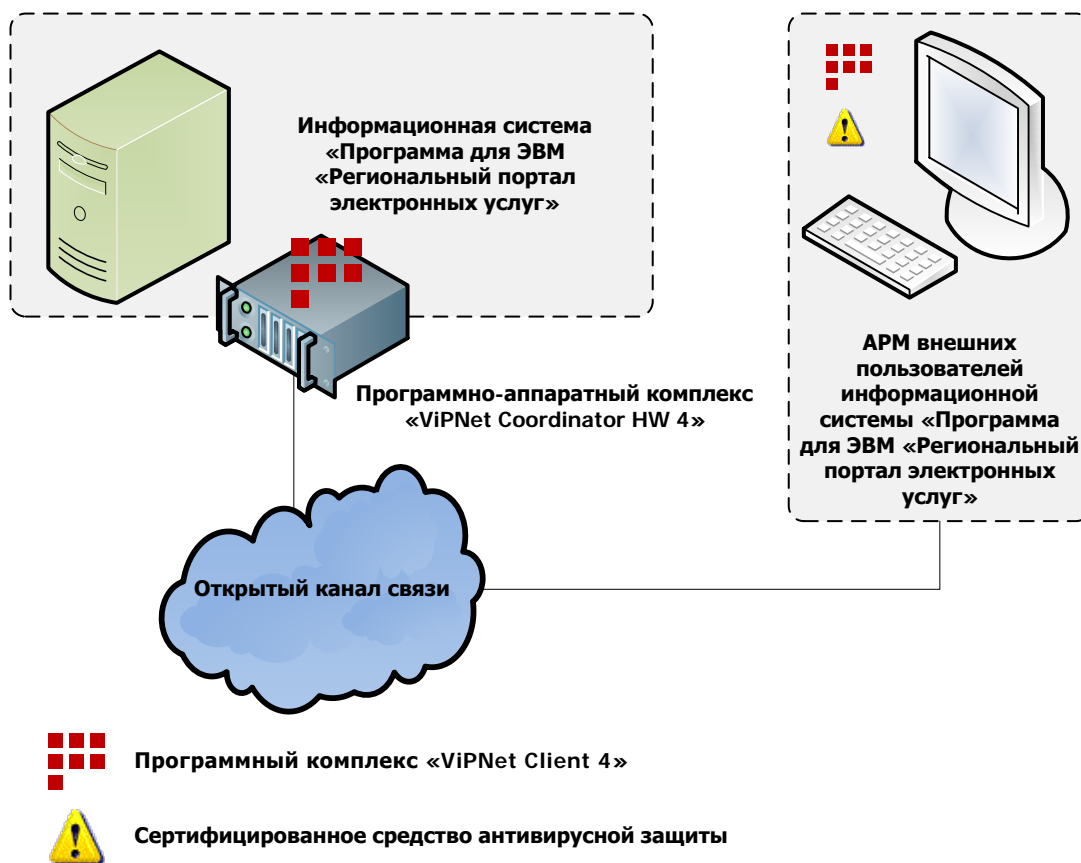


Рисунок 1

2. Порядок подключения внешних пользователей к защищенной сети Портала

Для подключения внешнего пользователя к Порталу необходимо выполнить следующие действия:

- согласование с Оператором подключения к Порталу;
- приобретение сертифицированного ФСБ России средства криптографической защиты информации (программный комплекс «ViPNet Client 4.x»);
- приобретение сертифицированного ФСТЭК России средства антивирусной защиты информации;
- отправка запроса Оператору на получение ПКИ;
- получение ПКИ;
- установка и настройка на АРМ внешних пользователей сертифицированного ФСБ России средства криптографической защиты информации (программный комплекс «ViPNet Client 4.x») и сертифицированного ФСТЭК России средства антивирусной защиты информации;
- разработка необходимой документации по эксплуатации криптографических средств в соответствии с требованиями нормативных документов ФСБ России.

После выполнения вышеуказанных действий необходимо уведомить Оператора о выполнении требований настоящего регламента.

При надлежащем выполнении требований Оператор принимает решение о предоставлении доступа к Порталу.

Содержание

СОДЕРЖАНИЕ	2
ПРИНЯТЫЕ СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ	3
НОРМАТИВНО-ПРАВОВЫЕ ССЫЛКИ	4
ВВЕДЕНИЕ	5
1. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПОДКЛЮЧЕНИИ ВНЕШНИХ ПОЛЬЗОВАТЕЛЕЙ К ПОРТАЛУ	6
2. ПОРЯДОК ПОДКЛЮЧЕНИЯ ВНЕШНИХ ПОЛЬЗОВАТЕЛЕЙ К ЗАЩИЩЕННОЙ СЕТИ ПОРТАЛА	8

Принятые сокращения и определения

АРМ	- автоматизированное рабочее место;
Портал	- информационная система «Программа для ЭВМ «Региональный портал электронных услуг» (ИС);
Внешние пользователи	- внешние пользователи информационной системы «Программа для ЭВМ «Региональный портал электронных услуг» (Органы власти, Органы местного самоуправления, многофункциональные центры)
НПА	- нормативный правовой акт;
ПКИ	- паролльно-ключевая информация;
Оператор	- Государственное учреждение «Новгородский информационно-аналитический центр»;
Регламент	- регламент подключения внешних пользователей к информационной системе «Программа для ЭВМ «Региональный портал электронных услуг» Государственного учреждения «Новгородский информационно-аналитический центр»;
СЗИ	- средства защиты информации;
СКЗИ	- средство криптографической защиты информации.

Нормативно-правовые ссылки

Настоящий документ разработан в соответствии со следующими нормативно-правовыми актами в области обеспечения безопасности информации:

[1] Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

[2] Приказ ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

[3] Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

[4] Приказ ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

[5] Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

[6] Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Введение

Настоящий документ разработан в соответствии с НПА [1]-[6] и регламентирует порядок подключения внешних пользователей к защищенной сети Портала, а также определяет обязательные технические и организационные требования по обеспечению информационной безопасности при подключении внешних пользователей к Порталу.

1. Требования по обеспечению информационной безопасности при подключении внешних пользователей к Порталу

1.1 Общие положения

В соответствии с НПА [1]-[6], информационное взаимодействие внешних пользователей с Оператором должно осуществляться по защищенному каналу связи.

В целях реализации требований вышеуказанных НПА, подключение к Порталу производится с использованием сертифицированных средств защиты информации, обеспечивающих безопасное информационное взаимодействие внешних пользователей с Оператором.

1.2 Основные требования

Для реализации защищенного взаимодействия внешних пользователей с Оператором на АРМ внешних пользователей, подключающихся к Порталу, должны быть выполнены следующие требования:

- обеспечение безопасного межсетевого взаимодействия;
- обеспечение защиты конфиденциальности и целостности передаваемой по каналам связи информации;
- выполнение обязательных организационных мероприятий, необходимых при эксплуатации средств криптографической защиты информации в соответствии с требованиями нормативных документов ФСБ России.

1.3 Требования к реализации организационных мероприятий по обеспечению защиты информации.

Для реализации защищенного взаимодействия внешних пользователей с Оператором необходимо разработать, утвердить документацию по эксплуатации криптографических средств в соответствии с требованиями нормативных документов ФСБ России:

- «Приказ «Об утверждении перечня мер, направленных на выполнение требований законодательства Российской Федерации в области защиты информации с использованием средств криптографической защиты», который включает в себя следующие мероприятия:

- назначение ответственного пользователя криптосредств;
- утверждение инструкции ответственного пользователя криптосредств;
- утверждение перечня сотрудников, допущенных к работе с криптосредствами, предназначенными для обеспечения безопасности информации;
- утверждение инструкции пользователей криптосредств;
- утверждение перечня помещений, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств;
- утверждение перечня лиц, имеющих доступ в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств;

- утверждение порядка доступа в помещения, где размещены используемые криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств.

- утверждение формы журнала поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов;

- утверждение формы лицевого счета пользователя криптосредств. Реализация вышеуказанных требований достигается путем выполнения следующих технических и организационных мер по защите информации:

1.4 Схема информационного взаимодействия АРМ внешних пользователей с Порталом представлена на рисунке 1.

Взаимодействие внешних пользователей с Порталом производится согласно типовой схеме (рисунок 1).

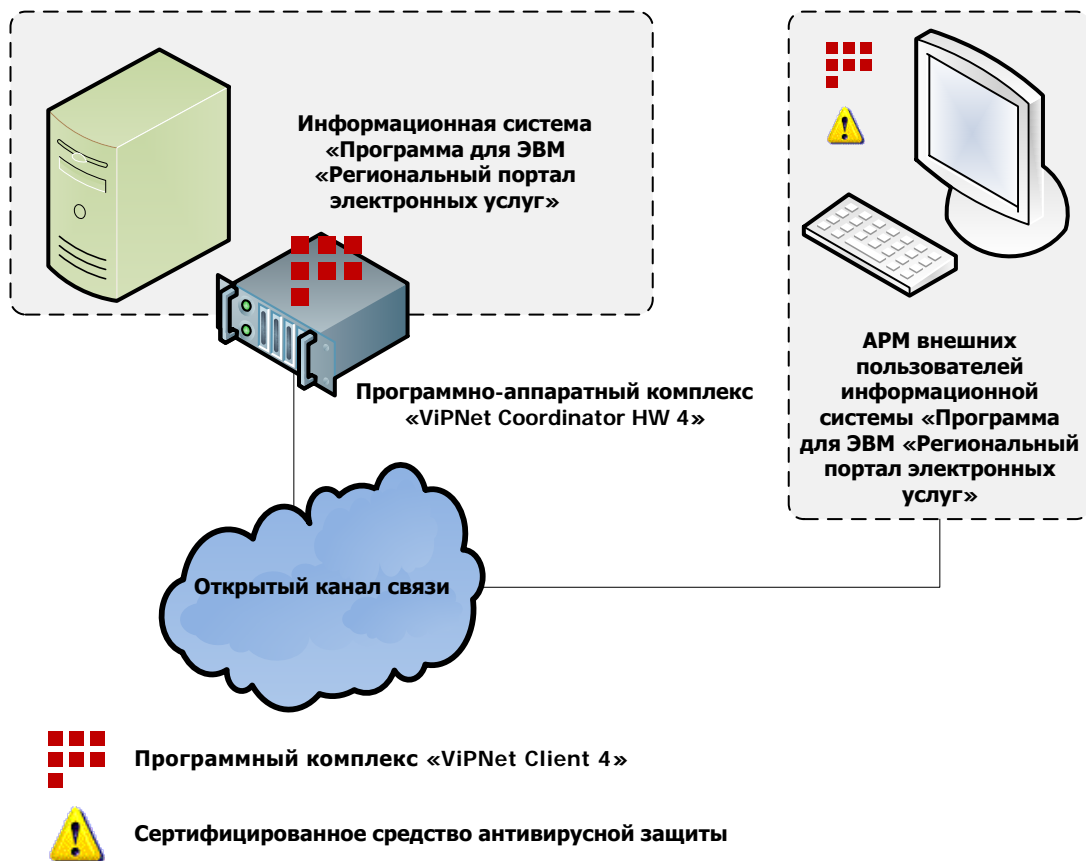


Рисунок 1

2. Порядок подключения внешних пользователей к защищенной сети Портала

Для подключения внешнего пользователя к Порталу необходимо выполнить следующие действия:

- Подать заявку Оператору на подключение к Порталу (Приложение 1).
- Приобретение сертифицированного ФСБ России СКЗИ (программный комплекс «ViPNet Client 4.x»). Приобретать программный комплекс «ViPNet Client 4.x» необходимо для сети Оператора (сеть № 2113)
- Приобретение сертифицированного ФСТЭК России средства антивирусной защиты информации.
- Отправить запрос на получение ПКИ оператору сети ViPNet (Приложение 2).
- Получить ПКИ. При приобретении «ViPNet Client» для сети Оператора, ответственному пользователю криптосредств необходимо явиться к Оператору и получить ПКИ.
- Установить и настроить на АРМ внешних пользователей сертифицированное ФСБ России СКЗИ.
- Установить и настроить на АРМ внешних пользователей сертифицированное ФСТЭК России средства антивирусной защиты информации.
- Разработать и утвердить необходимую документацию по эксплуатации криптографических средств в соответствии с требованиями нормативных документов ФСБ России.
- Провести оценку полноты выполнения мер по защите информации. Перед проведением оценки полноты выполнения мер, внутренним приказом создать комиссию по оценке полноты выполненных мер (Приложение 3). По завершению мероприятия, составить акт (Приложение 4) и направить Оператору.

При надлежащем выполнении требований Оператор принимает решение о предоставлении доступа к Порталу. После выполнения вышеуказанных действий необходимо уведомить Оператора о выполнении требований настоящего регламента.

При надлежащем выполнении требований Оператор принимает решение о предоставлении доступа к Порталу.

Приложение № 1
к Регламенту подключения внешних
пользователей к информационной системе
«Программа для ЭВМ «Региональный портал
электронных услуг» Государственного
учреждения «Новгородский информационно-
аналитический центр»

**Типовая форма Заявки
на подключение к информационной системе «Программа для ЭВМ
«Региональный портал электронных услуг» Государственного учреждения
«Новгородский информационно-аналитический центр»**

1. Полное наименование организации
2. Сокращенное название организации
3. Юридический адрес организации
4. Фактический (почтовый) адрес организации
5. ФИО руководителя
6. Должность руководителя
7. Количество Абонентских пунктов
8. Наименование Абонентских пунктов
9. ФИО ответственного за подключение
10. Контактные телефоны доверенного лица
11. Контактный E-mail доверенного лица

Приложение № 2
к Регламенту подключения внешних
пользователей к информационной системе
«Программа для ЭВМ «Региональный
портал электронных услуг»
Государственного учреждения
«Новгородский информационно-
аналитический центр»

**Запрос
на получение парольно-ключевой информации**

г.Великий Новгород

«___» _____ 20__ г.

В соответствии с регламентом подключения внешних пользователей к информационной системе к информационной системе «Программа для ЭВМ «Региональный портал электронных услуг» Государственного учреждения «Новгородский информационно-аналитический центр» (Далее – Портал) _____

(наименование организации)

провела мероприятия по выполнению организационных и технических требований для подключения к Порталу.

В соответствии с порядком подключения внешних пользователей к Порталу, прошу предоставить парольно-ключевую информацию для подключения к сети с номером 2113.

Руководитель организации _____ /

ФИО /

М.П.

Приложение № 3
к Регламенту подключения внешних
пользователей к информационной системе
«Программа для ЭВМ «Региональный
портал электронных услуг»
Государственного учреждения
«Новгородский информационно-
аналитический центр»

**Типовая форма Приказа «О комиссии по оценке полноты выполнения мер,
необходимых к применению согласно нормативным правовым актам по
обеспечению защиты информации»**

ПРИКАЗ

В целях выполнения требований Приказа ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Приказа ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» ПРИКАЗЫВАЮ:

1. Создать комиссию по оценке полноты выполнения мер, необходимых к применению согласно нормативным правовым актам по обеспечению защиты информации, (далее – Комиссия) в составе:

Председатель комиссии:

Члены комиссии:

2. Комиссии обеспечить проведение работ по оценке полноты выполнения мер, необходимых к применению согласно нормативным правовым актам по защите информации, в соответствии с «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденными приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21.

3. Контроль за исполнением настоящего приказа оставляю за собой.

Приложение № 4
к Регламенту подключения внешних
пользователей к информационной системе
«Программа для ЭВМ «Региональный портал
электронных услуг» Государственного
учреждения «Новгородский информационно-
аналитический центр»

**Акт
оценки полноты выполнения мер по защите информации**

г. Великий Новгород

« ___ » _____ 20__ г.

Составлен комиссией:

председатель – _____

члены комиссии: _____

Комиссия провела проверку выполнения технических и организационных мер по созданию _____ защищенного _____ канала _____ связи

« _____

(наименование организации)

_____» (далее – Организация)

с информационной системой «Программа для ЭВМ «Региональный портал электронных услуг» Государственного учреждения «Новгородский информационно-аналитический центр» (далее – Портал).

Комиссия выявила в Организации следующие средства защиты информации:

1. Средство криптографической защиты информации:

1.1. _____:

(наименование средства защиты)

Регистрационный номер – « _____ »;

Учетный номер СКЗИ – « _____ ».

2. Средство антивирусной защиты информации:

2.1. _____:

(наименование средства защиты)

Серийный номер – « _____ »;

Серийный номер – « _____ »;

Акт установки и готовности к вводу в эксплуатацию средств защиты информации (в том числе криптографических) № _____;

Разработан и утверждён комплект документации по эксплуатации криптографических средств в соответствии с требованиями нормативных документов ФСБ России

Комиссия сообщает:

о готовности « _____

(наименование организации)

_____» к подключению к Порталу.

Составлен в 2-х экземплярах.

Председатель комиссии: _____

Члены комиссии: _____
