



**НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ**

**Методические рекомендации  
по разработке Плана реагирования на компьютерные инциденты и  
принятия мер по ликвидации последствий компьютерных атак,  
проведенных в отношении значимых объектов критической  
информационной инфраструктуры Российской Федерации**

Москва, 2020

**СОДЕРЖАНИЕ**

1. Общие положения.....	3
2. Раздел «1. Технические характеристики и состав значимых объектов КИИ».....	6
3. Раздел «2. События (условия), при наступлении которых начинается реализация предусмотренных Планом мероприятий».....	6
4. Раздел «3. Подразделения и должностные лица, ответственные за проведение мероприятий по реагированию на компьютерные инциденты и принятие мер по ликвидации последствий компьютерных атак».....	8
5. Раздел «4. Мероприятия, проводимые в ходе реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, а также время, отводимое на их реализацию».....	9
6. Раздел «5. Условия привлечения подразделений и должностных лиц ФСБ России к проведению мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак».....	12
7. Раздел «6. Порядок проведения мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак в отношении значимого объекта КИИ совместно с привлекаемыми подразделениями и должностными лицами ФСБ России».....	13
Приложение 1. Дополнительные технические характеристики и параметры состава значимого объекта КИИ.....	16
Приложение 2. Описание состава подразделений и должностных лиц субъекта КИИ.....	18

## 1. Общие положения

1.1. Настоящие Методические рекомендации разработаны в целях методического обеспечения деятельности субъектов критической информационной инфраструктуры (далее – КИИ, субъекты КИИ соответственно), которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты КИИ, при разработке Плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак на значимые объекты критической информационной инфраструктуры (далее – План).

1.2. Методические рекомендации определяют общую структуру Плана, основные положения его разделов и содержат рекомендации по их составлению.

Методические рекомендации не содержат разъяснений условий привлечения подразделений и должностных лиц Банка России к проведению мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак в соответствии с пунктом 9 Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведённых в отношении значимых объектов критической информационной инфраструктуры Российской Федерации (далее – Порядок), утверждённого приказом ФСБ России от 19 июня 2019 г. № 282 (зарегистрирован Минюстом России 16 июля 2019 г., регистрационный № 55284).

1.3. Термины и определения употребляются в настоящих Методических рекомендациях в значениях, определенных Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», за исключением случаев, указанных особо.

1.4. При разработке Плана субъект КИИ включает в него мероприятия по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак таким образом, чтобы их реализация осуществлялась наиболее эффективно с учетом организационной структуры субъекта КИИ, а также назначения, архитектуры значимого объекта КИИ, применяемых

программных и программно-аппаратных средств, взаимодействия с другими объектами КИИ, наличия и характеристик доступа к сетям связи.

Утверждение настоящих Методических рекомендаций в качестве Плана не допускается.

1.5. Включаемые субъектом КИИ в План в обязательном порядке сведения содержатся в пункте 6 Порядка.

Указанные сведения рекомендуется включать в План в составе следующих разделов:

«1. Технические характеристики и состав значимых объектов КИИ.

2. События (условия), при наступлении которых начинается реализация предусмотренных Планом мероприятий.

3. Подразделения и должностные лица, ответственные за проведение мероприятий по реагированию на компьютерные инциденты и принятие мер по ликвидации последствий компьютерных атак.

4. Мероприятия, проводимые в ходе реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, а также время, отводимое на их реализацию.».

1.6. При необходимости в План включаются дополнительные разделы:

«5. Условия привлечения подразделений и должностных лиц ФСБ России к проведению мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак.

6. Порядок проведения мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак в отношении значимых объектов КИИ совместно с привлекаемыми подразделениями и должностными лицами ФСБ России.».

Решение о необходимости включения разделов 5 и 6 в План принимается руководителем субъекта КИИ исходя из анализа состояния системы безопасности значимого объекта КИИ и объективной степени готовности подразделений и (или) должностных лиц субъекта КИИ, ответственных за проведение мероприятий по

реагированию на компьютерные инциденты и принятие мер по ликвидации последствий компьютерных атак, к проведению таких мероприятий в полном объеме.

1.7. Кроме того, в План могут быть включены:

- разделы или положения, касающиеся порядка пересмотра Плана;
- разделы или положения, содержащие информацию или реквизиты, которые являются обязательными при составлении локальных нормативных актов в соответствии с правилами ведения делопроизводства субъекта КИИ;
- иные необходимые для реализации Плана разделы или положения.

1.8. В случае наличия у субъекта КИИ территориально распределенных значимых объектов КИИ, принадлежащих, в том числе, дочерним и зависимым обществам, допускается составление системы взаимоувязанных Планов при координирующей роли основного хозяйственного общества.

1.9. На согласование в ФСБ России в соответствии с пунктом 8 Порядка направляется проект Плана, содержащий разделы 5 и 6, до его утверждения.

Проект плана, не содержащий разделы 5 и 6, направлению на согласование в ФСБ России не подлежит. После утверждения такой план рекомендуется в порядке информирования направлять в Национальный координационный центр по компьютерным инцидентам (НКЦКИ) в кратчайшие сроки.

1.10. Субъектом КИИ могут вноситься изменения в План, в том числе по результатам тренировки по отработке содержащихся в нем мероприятий. При этом изменения в разделы 5 и 6 Плана вносятся по согласованию с ФСБ России. Об изменениях в План, не содержащий разделов 5 и 6, рекомендуется извещать НКЦКИ в кратчайшие сроки.

1.11. Субъект КИИ при реагировании на компьютерный инцидент может обратиться в НКЦКИ за консультативной помощью, используя контактные данные, указанные на официальном сайте в информационно-телекоммуникационной сети «Интернет» по адресу: «<http://cert.gov.ru>» или в рамках заключенных соглашений (регламентов).

## 2. Раздел «1. Технические характеристики и состав значимых объектов КИИ»

2.1. В данном разделе указывается информация, содержащаяся в Сведениях о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости, которые в соответствии с пунктом 18 постановления Правительства Российской Федерации от 8 февраля 2018 г. № 127 направлялись субъектом КИИ в ФСТЭК России по форме, утвержденной приказом ФСТЭК России от 22 декабря 2017 г. № 236 (зарегистрирован Минюстом России 13 апреля 2018 г., регистрационный № 50753), и по результатам проверки внесены ФСТЭК России в реестр значимых объектов КИИ.

2.2. Помимо информации, указанной в пункте 2.1 настоящих Методических рекомендаций, в целях наиболее эффективной организации деятельности по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак, в данном разделе рекомендуется указывать дополнительные технические характеристики и параметры состава значимого объекта КИИ.

Примеры дополнительных технических характеристик и параметров состава значимого объекта КИИ приведены в Приложении 1 к Методическим рекомендациям.

## 3. Раздел «2. События (условия), при наступлении которых начинается реализация предусмотренных Планом мероприятий»

3.1. Реализация предусмотренных Планом мероприятий начинается субъектом КИИ при получении информации о возникновении компьютерного инцидента, связанного с функционированием значимого объекта КИИ.

Субъектом КИИ определяются должностные лица, которыми могут приниматься решения о необходимости реализации мероприятий, предусмотренным планом.

Исходными данными при этом могут являться сведения о нарушениях функционирования и (или) безопасности элементов значимого объекта КИИ,

поступающие от сотрудников субъекта КИИ, а также технических средств мониторинга событий безопасности.

3.2. Для эффективного выявления фактов возникновения компьютерного инцидента субъектам КИИ рекомендуется определить порядок информирования должностных лиц, ответственных за проведение мероприятий по реагированию на компьютерные инциденты, связанные с функционированием значимого объекта КИИ, и принятие мер по ликвидации последствий направленных на него компьютерных атак (определены в разделе 4), о событиях (условиях), свидетельствующих о возникновении компьютерного инцидента, связанного с функционированием значимого объекта КИИ.

При этом источниками таких сведений могут выступать:

- сотрудники структурного подразделения субъекта КИИ, ответственного за обеспечение безопасности значимого объекта КИИ;

- сотрудники структурного подразделения субъекта КИИ, ответственного за эксплуатацию и (или) обеспечение функционирования значимого объекта КИИ, или сотрудники иной организации, выполняющие функции по эксплуатации и (или) обеспечению функционирования значимого объекта КИИ в силу заключенного с субъектом КИИ договора;

- сотрудники структурного подразделения субъекта КИИ, ответственного за эксплуатацию средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, и (или) за осуществление анализа результатов функционирования этих средств, или сотрудники иной организации, выполняющие указанные функции в силу заключенного с субъектом КИИ договора;

- НКЦКИ.

3.3. Событиями (условиями), свидетельствующими о возникновении компьютерного инцидента, связанного с функционированием значимого объекта КИИ, могут являться:

- нарушение установленного в организации режима доступа к информации или компонентам значимого объекта КИИ;

- функционирование вредоносного программного обеспечения<sup>1</sup> (далее – ВПО);
- несанкционированное изменение информации на элементах значимого объекта КИИ;
- превышение допустимой нагрузки на вычислительные ресурсы элементов значимого объекта КИИ;
- нарушение штатного режима функционирования сетевых сервисов элементов значимого объекта КИИ;
- исчерпание пропускной способности канала связи с элементами значимого объекта КИИ;
- отказ функционирующего на элементах значимого объекта КИИ программного и аппаратного обеспечения;
- иные нарушения в работе элементов значимого объекта КИИ, вызывающих прекращение выполнения его целевых функций.

Перечень событий (условий), свидетельствующих о возникновении компьютерного инцидента, может дополняться и актуализироваться в зависимости от целевых функций, архитектуры, параметров эксплуатации, применяемых средств защиты и других факторов. Отслеживание наступления таких событий (условий) рекомендуется осуществлять в том числе с помощью средств мониторинга событий информационной безопасности.

#### 4. Раздел «3. Подразделения и должностные лица, ответственные за проведение мероприятий по реагированию на компьютерные инциденты и принятие мер по ликвидации последствий компьютерных атак»

4.1. Субъектом КИИ определяются подразделения и (или) должностные лица (должностное лицо), ответственные за проведение мероприятий по реагированию на

---

<sup>1</sup> Вредоносное программное обеспечение – исполняемый программный код или набор интерпретируемых инструкций, заведомо предназначенный для нанесения вреда (ущерба) обладателю информации, хранящейся на средстве вычислительной техники, путём её несанкционированного копирования, уничтожения, модификации, блокирования или нейтрализации используемых на средстве вычислительной техники средств защиты, или для получения доступа к вычислительным ресурсам самого средства вычислительной техники с целью их несанкционированного использования.

компьютерные инциденты, связанные с функционированием значимого объекта КИИ, и принятие мер по ликвидации последствий направленных на него компьютерных атак. При необходимости разрабатывается соответствующий локальный нормативный акт об определении (назначении) указанных подразделений и (или) должностных лиц субъекта КИИ.

4.2. В Плане указываются реквизиты акта, в соответствии с которым определены (назначены) подразделения и (или) должностные лица субъекта КИИ, а также приводится их описание в карточке, являющейся приложением к Плану (образец карточки приведен в Приложении 2 к Методическим рекомендациям).

4.3. При описании подразделений и должностных лиц, ответственных за проведение мероприятий по реагированию на компьютерные инциденты, связанные с функционированием значимых объектов КИИ, и принятие мер по ликвидации последствий направленных на него компьютерных атак, указываются:

- наименования подразделений субъекта КИИ, ответственных за проведение мероприятий по реагированию на компьютерные инциденты, связанные с функционированием значимых объектов КИИ, и принятие мер по ликвидации последствий направленных на него компьютерных атак;

- ФИО, должности, контактные данные, место размещения сотрудников субъекта КИИ и возложенные на них функции при проведении мероприятий по реагированию на компьютерные инциденты, связанные с функционированием значимых объектов КИИ, и принятии мер по ликвидации последствий направленных на него компьютерных атак.

## 5. Раздел «4. Мероприятия, проводимые в ходе реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, а также время, отводимое на их реализацию»

5.1. Перечень и состав конкретных мероприятий, проводимых субъектом КИИ в ходе реагирования на компьютерные инциденты и принятия мер по ликвидации

последствий компьютерных атак, разрабатывается с указанием времени, необходимого на реализацию указанных мероприятий, исходя из:

- состава и особенностей функционирования элементов значимого объекта КИИ;
- типа выявленного компьютерного инцидента;
- состава имеющихся у субъекта КИИ сил и средств, выделенных для проведения необходимых мероприятий;
- наличия или отсутствия взаимодействия значимого объекта КИИ с ведомственным (корпоративным) центром государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА);
- положений документов, регламентирующих порядок эксплуатации значимого объекта КИИ и меры по обеспечению его информационной безопасности;
- положений иных нормативных правовых актов и методических документов.

5.2. В состав проводимых субъектом КИИ в ходе реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак мероприятий рекомендуется включать следующие мероприятия:

5.2.1. Регистрация в системе учета субъекта КИИ сведений о зафиксированном компьютерном инциденте, связанном с функционированием значимого объекта КИИ. В состав указанных сведений могут быть включены:

5.2.1.1. Краткая характеристика события, связанного с возникновением компьютерного инцидента (перечень возможных событий приведен в пункте 3.3 настоящих Методических рекомендаций).

5.2.1.2. Дата и время фиксации компьютерного инцидента.

5.2.1.3. Описание компьютерного инцидента (включая хронологию принятых мер).

5.2.1.4. Связь с другими выявленными ранее компьютерными атаками и компьютерными инцидентами (при наличии).

5.2.1.5. Контактная информация должностных лиц субъекта КИИ для взаимодействия с ними по данному компьютерному инциденту.

5.2.1.6. Параметры компьютерного инцидента, зависящие от характеристики события (набор данных может изменяться в зависимости от ситуации, инцидента или полноты известной информации по компьютерному инциденту). В качестве параметров компьютерного инцидента могут указываться:

- доменное имя и IP-адрес объекта компьютерной атаки;
- доменные имена и IP-адреса субъектов компьютерной атаки;
- мощность компьютерной атаки (пакетов в секунду, байт в секунду, запросов в секунду).
- доменное имя и IP-адрес центра удаленного управления ВПО;
- значение криптографической хэш-функции для образца ВПО;
- тип, идентификатор ВПО, наименование бот-сети;
- образец ВПО;
- образец сообщения электронной почты, с которым получен модуль ВПО;
- тип сетевого сервиса, аутентификационная информация, для доступа к которому была получена субъектами атаки;
- идентификатор выявленной уязвимости.

Рекомендуется сформировать типовые перечни сведений, подлежащих сбору в ходе реагирования на компьютерный инцидент. Данные перечни должны учитывать различные типы компьютерных инцидентов. В качестве примера таких перечней можно использовать перечень технических параметров компьютерных инцидентов, предоставляемых в НКЦКИ.

5.2.2. Информирование НКЦКИ в соответствии с пунктом 4 Порядка о компьютерном инциденте не позднее 3 часов с момента его обнаружения.

5.2.3. Определение (локализация) вовлеченных в компьютерный инцидент элементов значимого объекта КИИ.

5.2.4. Фиксация и анализ связанных с возникновением компьютерного инцидента материалов.

5.2.5. Установление причин и условий возникновения компьютерного инцидента, его класса (типа), а также источника и канала его возникновения.

5.2.6. Разработка рекомендаций по восстановлению штатного режима функционирования значимого объекта КИИ, повышению уровня защищенности значимого объекта КИИ и недопущению возникновения с ним компьютерных инцидентов в дальнейшем.

5.2.7. Восстановление штатного режима функционирования значимого объекта КИИ и проверка его работоспособности после восстановления.

5.2.8. Информирование НКЦКИ о результатах проведенных мероприятий не позднее 48 часов после их завершения в соответствии с пунктом 14 Порядка.

5.2.9. Реализация рекомендаций по повышению уровня защищенности значимого объекта КИИ и недопущению возникновения связанных с его функционированием компьютерных инцидентов в дальнейшем.

## 6. Раздел «5. Условия привлечения подразделений и должностных лиц ФСБ России к проведению мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак»

6.1. Условиями привлечения подразделений и должностных лиц ФСБ России к проведению мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак являются следующие:

6.1.1. Компьютерный инцидент привёл к прекращению функционирования значимого объекта КИИ.

6.1.2. Выполненные должностными лицами субъекта КИИ мероприятия не позволили ликвидировать последствия компьютерного инцидента, связанного с функционированием значимого объекта КИИ (восстановить штатное функционирование значимого объекта КИИ).

6.1.3. В НКЦКИ направлено сообщение о компьютерном инциденте, связанном с функционированием значимого объекта КИИ с указанием в нем необходимости привлечения подразделений и должностных лиц ФСБ России и причин, по которым

выполненные должностными лицами субъекта КИИ мероприятия не позволили ликвидировать последствия компьютерного инцидента.

## 7. Раздел «6. Порядок проведения мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак в отношении значимого объекта КИИ совместно с привлекаемыми подразделениями и должностными лицами ФСБ России»

7.1. При выполнении условий, предусмотренных пунктами 6.1.1 и 6.1.2 Методических рекомендаций, должностное лицо, ответственное за организацию мероприятий по реагированию на компьютерный инцидент, связанный с функционированием значимого объекта КИИ, докладывает руководству субъекта КИИ о необходимости привлечения к проведению мероприятий по реагированию на компьютерный инцидент и принятию мер по ликвидации последствий компьютерных атак подразделений и (или) должностных лиц ФСБ России.

7.2. Решение о необходимости привлечения подразделений и должностных лиц ФСБ России к проведению мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак принимается руководством субъекта КИИ.

7.3. При получении информации о принятом решении привлечь подразделения и должностные лица ФСБ России к проведению мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак должностное лицо субъекта КИИ, ответственное за взаимодействие с подразделениями и должностными лицами ФСБ России по вопросам реагирования на компьютерные инциденты, в течение 30 минут с момента получения указанной информации выполняет следующие действия:

7.3.1. Вносит в соответствующие поля карточки компьютерного инцидента информацию о результатах выполненных мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак.

7.3.2. Вносит в карточку компьютерного инцидента отметку о принятом решении привлечь подразделения и должностных лиц ФСБ России к ликвидации последствий компьютерного инцидента с указанием следующих сведений:

- адрес объекта размещения, вовлеченного в компьютерный инцидент элемента значимого объекта КИИ;
- контактная информация лица, сообщившего об инциденте;
- контактная информация представителей, ответственных за обеспечение функционирования вовлеченного в компьютерный инцидент элемента значимого объекта КИИ;
- время обнаружения признаков компьютерного инцидента;
- состав элементов значимого объекта КИИ, вовлеченных в компьютерный инцидент;
- сведения о зафиксированных нарушениях штатного режима функционирования элементов значимого объекта КИИ;
- сведения о предпринятых мерах;
- сведения о динамике развития инцидента с учетом принятых мер;
- технические сведения о функционировании элементов значимого объекта КИИ (включая адреса расположения, схемы, состав, перечень используемых средств защиты информации, порядок сопряжения с внешними сетями и системами и т.д.);
- причины, по которым собственными силами ликвидация последствий компьютерного инцидента, связанного с функционированием значимого объекта КИИ, не представляется возможной.

7.3.3. Карточка компьютерного инцидента после заполнения направляется в НКЦКИ.

7.4. После получения от НКЦКИ подтверждения о привлечении подразделений и должностных лиц ФСБ России к мероприятиям по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак должностное лицо субъекта КИИ, ответственное за взаимодействие с подразделениями и должностными лицами ФСБ России по вопросам реагирования на

компьютерные инциденты, в целях организации работы привлекаемых подразделений и должностных лиц ФСБ России выполняет следующие действия:

7.4.1. Обеспечивает беспрепятственный доступ сотрудников ФСБ России к значимому объекту КИИ, с функционированием которого связан компьютерный инцидент.

7.4.2. Обеспечивает взаимодействие сотрудников ФСБ России с уполномоченными должностными лицами субъекта КИИ, эксплуатирующими вовлеченные в компьютерный инцидент элементы значимого объекта КИИ, по вопросам, возникающим в ходе реагирования на компьютерный инцидент.

7.4.3. Организует реализацию полученных от должностных лиц ФСБ России в ходе реагирования на компьютерный инцидент рекомендаций по ликвидации последствий компьютерного инцидента, повышению уровня защищенности значимого объекта КИИ, с функционированием которого был связан компьютерный инцидент, и недопущению возникновения таких компьютерных инцидентов в дальнейшем.

**Дополнительные технические характеристики и параметры состава значимого  
объекта КИИ**

**1. Описание (технические характеристики) значимого объекта КИИ**

<b>Сведения о наличии средств архивирования и резервного копирования данных.</b>	Средства архивирования и резервного копирования отсутствуют.
<b>Сведения о подключении значимого объекта КИИ к корпоративному (ведомственному) центру ГосСОПКА</b>	Значимый объект КИИ к корпоративному (ведомственному) центру ГосСОПКА не подключен.
<b>Сведения об установленных на значимом объекте КИИ средствах ГосСОПКА</b>	Средства ГосСОПКА на значимом объекте КИИ не установлены.

## 2. Состав значимого объекта КИИ

№ п/п	Наименование элемента значимого объекта КИИ	Сетевое имя	Провайдер	Доменное имя	Внешний IP-адрес	Внутренний IP-адрес	Используемые протоколы	ОС <sup>2</sup>	ППО <sup>3</sup>	Название учетных записей	Лицо, ответственное за эксплуатацию <sup>4</sup>	Лицо, ответственное за администрирование <sup>4</sup>	Средства защиты
1.	Коммутатор (модель)	hp	ООО «Связь»	–	–	192.168.0.1	tcp, udp, snmp, ssh	–	–	admin	9	8	–
2.	Сервер (модель)	serv	–	–	–	192.168.0.2	tcp, udp, ssh	ОС (наименование, версия)	ППО (наименование, версия)	root user1-user15	9	8	АВС <sup>5</sup> (наименование, версия)
3.	СВТ (модель)	user1	–	–	–	192.168.0.3	tcp, udp,	ОС (наименование, версия)	ППО (наименование, версия)	user1	9	8	АВС (наименование, версия)
4.	СВТ (модель)	user2	–	–	–	192.168.0.4	tcp, udp,	ОС (наименование, версия)	ППО (наименование, версия)	user2	9	8	АВС (наименование, версия)
5.	СВТ (модель)	user3	–	–	–	192.168.0.5	tcp, udp,	ОС (наименование, версия)	ППО (наименование, версия)	user3	9	8	АВС (наименование, версия)
6.	СВТ (модель)	user4	–	–	–	192.168.0.6	tcp, udp,	ОС (наименование, версия)	ППО (наименование, версия)	user4	9	8	АВС (наименование, версия)
7.	СВТ (модель)	user5	–	–	–	192.168.0.7	tcp, udp,	ОС (наименование, версия)	ППО (наименование, версия)	user5	9	8	АВС (наименование, версия)

<sup>2</sup> Операционная система.

<sup>3</sup> Прикладное программное обеспечение.

<sup>4</sup> Указывается номер строки таблицы Приложения 2 в которой содержатся сведения о соответствующем должностном лице.

<sup>5</sup> Антивирусное средство.

### Описание состава подразделений и должностных лиц субъекта КИИ

№ п/п	ФИО	Должность	Функции	Контактные данные	Место размещения
<b>Руководство субъекта КИИ</b>					
1.	ФИО	Руководитель (заместитель руководителя) субъекта КИИ	Принимает решение о привлечении к мероприятиям должностных лиц и подразделений ФСБ России	8-495-111-11-01 8-916-111-11-01 1@zokii.ru	каб. № 1
<b>Отдел обеспечения информационной безопасности значимого объекта КИИ</b>					
2.	ФИО	Начальник отдела	Ответственный за организацию мероприятий, контроль деятельности участвующих в мероприятиях должностных лиц Субъекта	8-495-111-11-02 8-916-111-11-02 2@zokii.ru	каб. № 2
3.	ФИО	Заместитель начальника отдела	Ответственный за взаимодействие с подразделениями и должностными лицами ФСБ России, привлекаемыми к проведению мероприятий	8-495-111-11-03 8-916-111-11-03 3@zokii.ru	каб. № 3
4.	ФИО	Старший инженер	Ответственный за проведение анализа полученных в ходе проведенных мероприятий материалов	8-495-111-11-04 8-916-111-11-04 4@zokii.ru	каб. № 4
5.	ФИО	Инженер	Ответственный за сбор в ходе проводимых мероприятий материалов	8-495-111-11-05 8-916-111-11-05 5@zokii.ru	каб. № 5
6.	ФИО	Инженер	Ответственный за формирование рекомендаций по повышению защищенности значимого объекта КИИ и недопущению возникновения с ним компьютерных инцидентов в дальнейшем	8-495-111-11-06 8-916-111-11-06 6@zokii.ru	каб. № 6

№ п/п	ФИО	Должность	Функции	Контактные данные	Место размещения
<b>Отдел эксплуатации и обеспечения функционирования значимого объекта КИИ</b>					
7.	ФИО	Старший инженер	Ответственный за проведение инвентаризации значимого объекта КИИ и ее предоставление привлекаемым к мероприятиям сотрудникам	8-495-111-11-07 8-916-111-11-07 7@zokii.ru	каб. № 7
8.	ФИО	Старший инженер	Ответственный за администрирование значимого объекта КИИ	8-495-111-11-08 8-916-111-11-08 8@zokii.ru	каб. № 8
9.	ФИО	Инженер	Ответственный за эксплуатацию значимого объекта КИИ	8-495-111-11-9 8-916-111-11-9 9@zokii.ru	каб. № 9
10.	ФИО	Инженер	Ответственный за реализацию рекомендаций по повышению защищенности значимого объекта КИИ и недопущению возникновения с ним компьютерных инцидентов в дальнейшем	8-495-111-11-10 8-916-111-11-10 10@zokii.ru	каб. № 10