ВЫПИСКА ИЗ КОНЦЕПЦИИ
государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

(Концепция утверждена Президентом Российской Федерации 12 декабря 2014 г. № К 1274)

I. Общие положения

1. Настоящей Концепцией определяются назначение, функции и принципы создания государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее - Система), а также виды обеспечения, необходимые для ее создания и функционирования.

2. Система представляет собой единый централизованный, территориально распределенный комплекс, включающий силы и средства обнаружения, предупреждения и ликвидации последствий компьютерных атак, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, и федеральный орган исполнительной власти, уполномоченный в области создания и обеспечения функционирования Системы.

4. Правовую основу настоящей Концепции составляют Конституция Российской Федерации, федеральные законы, Стратегия национальной безопасности Российской Федерации до 2020 года, Доктрина информационной безопасности Российской Федерации, Указ Президента Российской Федерации от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» и иные нормативные правовые акты Российской Федерации.

5. В настоящей Концепции используются следующие основные понятия:

а) субъекты Системы - федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской

Федерации, федеральный орган исполнительной власти, уполномоченный в области создания и обеспечения функционирования Системы, владельцы информационных ресурсов Российской Федерации, операторы связи, а также иные организации, осуществляющие лицензируемую деятельность в области защиты информации;

б) зона ответственности субъекта Системы - совокупность информационных ресурсов Российской Федерации, в отношении которых субъектом Системы обеспечиваются обнаружение, предупреждение и ликвидация последствий компьютерных атак;

в) силы обнаружения, предупреждения и ликвидации последствий компьютерных атак - уполномоченные подразделения субъектов Системы и специально выделенные сотрудники субъектов Системы, принимающие участие в обнаружении, предупреждении и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

г) средства обнаружения, предупреждения и ликвидации последствий компьютерных атак - технологии, а также технические, программные, лингвистические, правовые, организационные средства, включая сети и средства связи, средства сбора и анализа информации, поддержки принятия управленческих решений (ситуационные центры), предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

II. Назначение, функции, принципы создания и функционирования Системы

6. Основным назначением Системы является обеспечение защищенности информационных ресурсов Российской Федерации от компьютерных атак и штатного функционирования данных ресурсов в условиях возникновения компьютерных инцидентов, вызванных компьютерными атаками.

7. Для выполнения основных задач, определенных в Указе Президента Российской Федерации от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные

ресурсы Российской Федерации», Система осуществляет реализацию следующих функций:

а) выявление признаков проведения компьютерных атак, определение их источников, методов, способов и средств осуществления и направленности, а также разработка методов и средств обнаружения, предупреждения и ликвидации последствий компьютерных атак;

б) формирование и поддержание в актуальном состоянии детализированной информации об информационных ресурсах Российской Федерации, находящихся в зоне ответственности субъектов Системы;

в) прогнозирование ситуации в области обеспечения информационной безопасности Российской Федерации, включая выявленные и прогнозируемые угрозы и их оценку;

г) организация и осуществление взаимодействия с правоохранительными органами и другими государственными органами, владельцами информационных ресурсов Российской Федерации, операторами связи, интернет-провайдерами и иными заинтересованными организациями на национальном и международном уровнях в области обнаружения компьютерных атак и установления их источников, включая обмен информацией о выявленных компьютерных атаках и вызванных ими компьютерных инцидентах, а также обмен опытом в сфере выявления и устранения уязвимостей программного обеспечения и оборудования и реагирования на компьютерные инциденты;

д) организация и проведение научных исследований в сфере разработки и применения средств и методов обнаружения, предупреждения и ликвидации последствий компьютерных атак;

е) осуществление мероприятий по обеспечению подготовки и повышения квалификации кадров, требующихся для создания и функционирования Системы;

ж) сбор и анализ информации о компьютерных атаках и вызванных ими компьютерных инцидентах в отношении информационных ресурсов Российской Федерации, а также о компьютерных инцидентах в информационных системах и информационно-телекоммуникационных сетях других стран, с которыми взаимодействуют владельцы информационных ресурсов Российской Федерации;

з) осуществление мероприятий по оперативному реагированию на компьютерные атаки и вызванные ими компьютерные инциденты, а также по ликвидации последствий данных компьютерных инцидентов в информационных ресурсах Российской Федерации;

и) выявление, сбор и анализ сведений об уязвимостях программного обеспечения и оборудования;

к) мониторинг степени защищенности информационных систем и информационно-телекоммуникационных сетей на всех этапах создания, функционирования и модернизации информационных ресурсов Российской Федерации, а также разработка методических рекомендаций по организации защиты информационных ресурсов Российской Федерации от компьютерных атак;

м) организация и осуществление антивирусной защиты;

н) совершенствование оперативно-тактического взаимодействия сил и средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

8. Создание и функционирование Системы осуществляется на основе следующих принципов:

а) территориальная распределенность Системы;

б) отраслевая и территориальная организация Системы;

в) единство государственного планирования, а также координации и контроля реализации комплекса технических и организационных мер;

г) обеспечение функционирования Системы на основе единой научно-технической и организационно-методической политики;

д) достаточность и рациональное использование сил и средств обнаружения, предупреждения и ликвидации последствий компьютерных атак;

е) разделение полномочий и ответственности между субъектами Системы на основе нормативно-правовой базы Российской Федерации.

III. Организационные основы Системы

9. Основной организационно-технической составляющей Системы являются центры обнаружения, предупреждения и ликвидации последствий компьютерных атак (далее - центры),

организованные по ведомственному и территориальному принципам.

10. К основным задачам центров относятся:

а) обнаружение, предупреждение и ликвидация последствий компьютерных атак, направленных на контролируемые информационные ресурсы;

б) проведение мероприятий по оценке степени защищенности контролируемых информационных ресурсов;

в) проведение мероприятий по установлению причин компьютерных инцидентов, вызванных компьютерными атаками на контролируемые информационные ресурсы;

г) сбор и анализ данных о состоянии информационной безопасности в контролируемых информационных ресурсах;

д) осуществление взаимодействия между центрами;

е) информирование заинтересованных лиц и субъектов Системы по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак.

11. Центры подразделяются на главный центр Системы, региональные центры, территориальные центры, центры органов государственной власти Российской Федерации и органов государственной власти субъектов Российской Федерации (далее - ведомственные центры) и корпоративные центры.

12. Главный центр Системы, региональные и территориальные центры Системы создаются силами федерального органа исполнительной власти, уполномоченного в области создания и обеспечения функционирования Системы. Зоной ответственности данных центров являются информационные ресурсы органов государственной власти Российской Федерации и органов государственной власти субъектов Российской Федерации (далее - органы государственной власти), а также информационные ресурсы указанного федерального органа исполнительной власти.

Данные центры организуют и проводят в соответствии с законодательством Российской Федерации мероприятия по оценке степени защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак.

13. Ведомственные центры создаются заинтересованными органами государственной власти. Зоной ответственности таких центров являются принадлежащие органам государственной власти информационные ресурсы. Также ведомственные центры могут

создаваться и эксплуатироваться в интересах органов государственной власти организациями, осуществляющими лицензируемую деятельность в области защиты информации.

Функционирование ведомственного центра обеспечивается органом государственной власти, создавшим этот центр.

14. Корпоративные центры могут создаваться государственными корпорациями, операторами связи и другими организациями, осуществляющими лицензируемую деятельность в области защиты информации.

Функционирование корпоративного центра обеспечивается организацией, создавшей такой центр.

15. Включение ведомственного (корпоративного) центра в состав Системы осуществляется на основе соглашения органа государственной власти (организации), создавшего (создавшей) указанный центр, с федеральным органом исполнительной власти, уполномоченным в области создания и обеспечения функционирования Системы.

16. В составе Системы функционирует созданный в Федеральной службе безопасности Российской Федерации Национальный координационный центр по компьютерным инцидентам, который организует и осуществляет обмен информацией о компьютерных инцидентах с юридическими лицами, владеющими на праве собственности или ином законном основании объектами критической информационной инфраструктуры Российской Федерации, операторами связи, обеспечивающими взаимодействие объектов критической информационной инфраструктуры Российской Федерации между собой, уполномоченными органами иностранных государств, международными и неправительственными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты.

18. Федеральный орган исполнительной власти, уполномоченный в области создания и обеспечения функционирования Системы, осуществляет доведение до субъектов Системы информации об угрозах информационным ресурсам Российской Федерации и о необходимых мерах по нейтрализации данных угроз, а также обеспечивает реализацию мероприятий по совершенствованию оперативно-тактического взаимодействия субъектов Системы.

IV. Нормативно-правовое, научно-техническое, информационно-аналитическое, кадровое и организационно-штатное обеспечение создания и функционирования Системы

19. Нормативно-правовое обеспечение создания и функционирования Системы включает:

а) создание законодательной базы Российской Федерации;

б) порядок фиксации и обмена информацией между субъектами Системы о компьютерных атаках на информационные ресурсы Российской Федерации и вызванных ими компьютерных инцидентах;

в) порядок осуществления деятельности субъектов Системы в области обнаружения, предупреждения и ликвидации последствий компьютерных атак;

г) порядок и периодичность проведения мероприятий по оценке степени защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак;

д) порядок обмена информацией между органами государственной власти и уполномоченными органами иностранных государств (международными организациями) о компьютерных инцидентах.

20. Научно-техническое обеспечение создания и функционирования Системы осуществляется на основе результатов фундаментальных и прикладных научно-технических исследований и работ по следующим направлениям:

а) разработка методов выявления признаков проведения компьютерных атак, определения их источников и способов осуществления и направленности;

б) разработка методик проведения мероприятий по оценке степени защищенности информационных систем и информационно-телекоммуникационных сетей от компьютерных атак, фиксации компьютерных инцидентов, а также методических рекомендаций в области выявления, предупреждения и ликвидации последствий компьютерных атак, включая рекомендации по организации защиты критической информационной инфраструктуры Российской Федерации от компьютерных атак;

в) прогнозирование и разработка моделей в области обеспечения информационной безопасности Российской Федерации;

д) разработка методик обнаружения компьютерных атак на

информационные системы и информационно-телекоммуникационные сети;

е) разработка методов и средств выявления и предупреждения компьютерных инцидентов, вызванных компьютерными атаками.

21. Информационно-аналитическое обеспечение функционирования Системы осуществляется на основе прогнозирования ситуации в области обеспечения информационной безопасности Российской Федерации. Исходными данными для прогнозирования являются:

а) информация, получаемая средствами обнаружения, предупреждения и ликвидации последствий компьютерных атак;

б) результаты оценки степени защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак;

в) информация о компьютерных атаках и вызванных ими компьютерных инцидентах, поступающая по каналам международного обмена.

22. Кадровое и организационно-штатное обеспечение создания и функционирования Системы включает:

а) целевое выделение дополнительных штатных ресурсов заинтересованным органам государственной власти;

б) совершенствование нормативно-методического обеспечения подготовки, переподготовки и повышения квалификации кадров, обеспечивающих реализацию функций Системы;

в) развитие учебно-лабораторной базы подготовки, переподготовки и повышения квалификации кадров, обеспечивающих реализацию функций Системы;

г) подготовку, переподготовку и повышение квалификации кадров, обеспечивающих реализацию функций Системы.