ДЕПАРТАМЕНТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ САМАРСКОЙ ОБЛАСТИ

ПРИКАЗ

от 15.10.2021 № 93-п

Об утверждении Положения о центре обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные системы и ресурсы Самарской области и Регламента деятельности центра обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные системы и ресурсы Самарской области

В соответствии с постановлением Правительства Самарской области от 20.11.2015 № 745 «О центре обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные системы и ресурсы Самарской области» ПРИКАЗЫВАЮ:

1. Утвердить:

Положение о центре обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные системы и ресурсы Самарской области в соответствии с приложением 1 к настоящему приказу;

Регламент деятельности центра обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные системы и ресурсы Самарской области в соответствии с приложением 2 к настоящему приказу.

2. Признать утратившими силу:

приказ департамента информационных технологий и связи Самарской области от 18.12.2015 № 90-п «Об утверждении Положения о Центре обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные системы и ресурсы Самарской области»;

абзац четвёртый пункта 1 приказа департамента информационных технологий и связи Самарской области от 07.05.2021 № 40-п «О внесении изменений в отдельные приказы департамента информационных технологий и связи Самарской области».

3. Опубликовать настоящий приказ в средствах массовой информации.

4. Настоящий приказ вступает в силу со дня его официального опубликования.

5. Контроль за исполнением настоящего приказа оставляю за собой.

Заместитель председателя
Правительства Самарской области –
руководитель департамента
информационных технологий и связи
Самарской области К.Г.Пресняков

Графинина 3351364

ПРИЛОЖЕНИЕ 1
к приказу департамента
информационных технологий
и связи Самарской области
от 15.10.2021 № 93-н

ПОЛОЖЕНИЕ
о центре обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные системы и ресурсы Самарской области

1. Общие положения

1.1. Настоящее Положение о центре обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные системы и ресурсы Самарской области (далее – Положение) определяет задачи, функции, зону ответственности центра обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные системы и ресурсы Самарской области (далее - Центр ГосСОПКА), а также требования к составу и характеристикам специалистов Центра ГосСОПКА в рамках деятельности, направленной на обнаружение, предупреждение, ликвидацию последствий компьютерных атак, реагирование на компьютерные инциденты и взаимодействие с Национальным координационным центром по компьютерным инцидентам (далее – НКЦКИ).

Краткое наименование Центра ГосСОПКА – Региональный Центр Кибербезопасности Самарской области.

1.2. Центр ГосСОПКА создан с целью обнаружения, предупреждения, ликвидации последствий компьютерных атак, реагирования на компьютерные инциденты в зоне своей ответственности.

1.3. Центр ГосСОПКА создан на базе государственного бюджетного учреждения Самарской области «Цифровой регион» (далее – Учреждение), находящегося в ведении департамента информационных технологий и связи Самарской области (далее – ДИТиС СО).

1.4. Центр ГосСОПКА подчиняется директору Учреждения.

1.5. Руководство Центром ГосСОПКА осуществляет один из руководителей структурных подразделений Учреждения либо заместитель директора Учреждения на основании приказа директора Учреждения.

1.6. Структура и штатная численность Центра ГосСОПКА определяются приказом директора Учреждения.

1.7. При осуществлении своей деятельности Центр ГосСОПКА руководствуется следующими документами:

Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

приказом Федеральной службы безопасности России (далее – ФСБ России) от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»;

приказом ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации»;

приказом ФСБ России от 19.06.2019 № 281 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак

и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации»;

приказом ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;

требованиями к подразделениям и должностным лицам субъектов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, утвержденными директором НКЦКИ;

методическими документами, разработанными НКЦКИ;

уставом Учреждения;

приказами ДИТиС СО и директора Учреждения.

1.8. Центр ГосСОПКА в соответствии с объемом выполняемых функций является Центром ГосСОПКА класса А.

1.9. Регламент деятельности Центра ГосСОПКА утверждается приказом ДИТиС СО.

2. Задачи Центра ГосСОПКА

2.1.Центр ГосСОПКА осуществляет свою деятельность с целью решения следующих задач:

обеспечение процессов обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты в зоне ответственности Центра ГосСОПКА;

развитие сил и средств Центра ГосСОПКА в соответствии с нормативно-

методическими документами в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

3. Функции, выполняемые Центром ГосСОПКА

3.1. С целью решения задач в зоне своей ответственности Центр ГосСОПКА реализует выполнение следующих функций:

1) взаимодействие с НКЦКИ при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы и реагирования на компьютерные инциденты, в том числе в части информационно-аналитического и прогностического обеспечения функционирования Центра ГосСОПКА, предоставление в НКЦКИ сведений о состоянии защищенности информационных ресурсов от компьютерных атак и информации о компьютерных инцидентах в соответствии с установленным порядком;

2) разработка документов, регламентирующих процессы обнаружения, предупреждения и ликвидации последствий компьютерных инцидентов и реагирования на компьютерные инциденты;

3) эксплуатация средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, выявление ошибок в работе средств и направление производителю средств информации о выявленных ошибках, а также актуализация средств, используемых для обеспечения защиты информационных ресурсов, направление в НКЦКИ предложений по совершенствованию средств;

4) прием сообщений об инцидентах от персонала и пользователей информационных ресурсов;

5) регистрация компьютерных атак и компьютерных инцидентов;

6) анализ событий информационной безопасности;

7) инвентаризация информационных ресурсов;

8) анализ угроз информационной безопасности, прогнозирование их развития и направление в НКЦКИ результатов;

9) составление и актуализация перечня угроз информационной безопасности для информационных ресурсов;

10) выявление уязвимостей информационных ресурсов;

11) формирование предложений по повышению уровня защищенности информационных ресурсов;

12) составление перечня компьютерных инцидентов;

13) ликвидация последствий компьютерных инцидентов;

14) анализ результатов ликвидации последствий инцидентов;

15) установление причин компьютерных инцидентов.

4. Зона ответственности Центра ГосСОПКА

4.1. Зоной ответственности Центра ГосСОПКА являются информационные ресурсы:

органов государственной власти Самарской области, а также подчиненных им структурных подразделений и подведомственных организаций (учреждений), органов местного самоуправления и подведомственных им организаций (учреждений), которые размещены на специализированной технологической площадке Учреждения и по которым переданы права на обнаружение, предупреждение и ликвидацию последствий компьютерных атак на информационные ресурсы и реагирования на компьютерные инциденты на основании соглашений, договоров, государственных (муниципальных) контрактов;

органов государственной власти Самарской области, а также подчиненных им структурных подразделений и подведомственных организаций (учреждений), органов местного самоуправления и подведомственных им организаций (учреждений), которые не размещены на специализированной технологической площадке Учреждения, но по которым переданы права на обнаружение, предупреждение и ликвидацию последствий

компьютерных атак на информационные ресурсы и реагирования на компьютерные инциденты на основании соглашений, договоров, государственных (муниципальных) контрактов;

иных органов и организаций, передавших в полном объеме либо частично права на обнаружение, предупреждение и ликвидацию последствий компьютерных атак на информационные ресурсы и реагирования на компьютерные инциденты на основании соглашений, договоров, государственных (муниципальных) контрактов;

государственные информационные системы Самарской области, оператором которых является Учреждение.

4.2. Зона ответственности Центра ГосСОПКА определяется при принятии решения о его создании и изменяется в процессе его функционирования в установленном настоящим Положением порядке.

4.3. При реализации мероприятий по включению и исключению из зоны ответственности Центра ГосСОПКА информационных ресурсов Центр ГосСОПКА письменно информирует НКЦКИ о результатах данных мероприятий.

4.4. Исключение защищаемых информационных ресурсов из зоны ответственности Центра ГосСОПКА не должно приводить к изменению полноты выполняемых мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных в отношении других информационных ресурсов, находящихся в зоне ответственности Центра ГосСОПКА.

5. Силы Центра ГосСОПКА

5.1. Состав специалистов Центра ГосСОПКА устанавливается штатным расписанием, утверждаемым приказом директора Учреждения.

5.2. Обязанности специалистов Центра ГосСОПКА определяются должностными инструкциями, утверждаемыми приказом директора Учреждения.

5.4. Специалисты должны удовлетворять требованиям к персоналу Центра ГосСОПКА, предъявляемым к ним в Требованиях к подразделениям и должностным лицам субъектов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, утверждённых ФСБ России от 26.04.2018 №149/2/7-322.

Штатное расписание и должностные инструкции специалистов Центра ГосСОПКА соответствуют ролям, приведенным в таблице 1.

Таблица 1 – Роли сотрудников Центра ГосСОПКА

Роль	**Функции**
Специалисты первой линии:	
Специалист по взаимодействию с персоналом и пользователями	Прием сообщений персонала и пользователей информационных ресурсов, подготовка информации для предоставления в НКЦКИ, взаимодействие с НКЦКИ
Специалист по обнаружению компьютерных атак и инцидентов	Анализ событий информационной безопасности, регистрация компьютерных атак и инцидентов, взаимодействие с НКЦКИ
Специалист по обслуживанию средств центра ГосСОПКА	Обеспечение функционирования средств, размещаемых в Центре ГосСОПКА, а также дополнительных средств защиты информационных систем
Специалисты второй линии:	
Специалист по оценке защищенности	Проведение инвентаризации информационных ресурсов, выявление уязвимостей, сбор и анализ выявленных уязвимостей и угроз, установление соответствия требований по информационной безопасности принимаемым мерам, взаимодействие с НКЦКИ
Специалист по ликвидации последствий компьютерных инцидентов	Координация действий при реагировании на компьютерные инциденты и приведение в штатный режим работы, взаимодействие с НКЦКИ
Специалист по установлению причин компьютерных инцидентов	Установление причин компьютерных инцидентов, анализ последствий инцидентов и подготовка перечня компьютерных инцидентов, взаимодействие с НКЦКИ

Специалисты третьей линии:	
Аналитик	Анализ информации, предоставляемой специалистами первой и второй линий; выявление и анализ угроз информационной безопасности, прогнозирование развития угроз; разработка предложений по доработке нормативных и методических документов по вопросам информационной безопасности, взаимодействие с НКЦКИ
Технический эксперт	Экспертная поддержка в соответствии со специализацией (вредоносное программное обеспечение, настройка средств защиты, применение специализированных технических средств, оценка защищенности и т.п.), формирование предложений по повышению уровня защищенности; разработка предложений по доработке нормативных и методических документов по вопросам информационной безопасности
Специалист	Нормативно-правовое и методическое сопровождение деятельности Центра ГосСОПКА
Руководитель	Управление деятельностью Центра ГосСОПКА, взаимодействие с НКЦКИ внесение изменений в соответствующие нормативные и методические документы.

6. Требования к персоналу Центра ГосСОПКА:

6.1. Руководитель и (или) лицо, уполномоченное руководить работой Центра ГосСОПКА, должен удовлетворять одному из следующих условий:

иметь высшее профессиональное образование по направлению подготовки «Информационная безопасность» в соответствии с Общероссийским классификатором специальностей и (или) пройти переподготовку по одной из специальностей данного направления (нормативный срок – не менее 360 часов), а также иметь стаж в области выполняемых Центром ГосСОПКА работ не менее 5 лет;

иметь высшее образование по направлению подготовки (специальности) в области математических и естественных наук, инженерного дела,

технологий и технических наук и стаж руководящей работы в сфере информационной безопасности не менее 10 лет.

6.2. Специалисты первой линии должны удовлетворять одному из следующих условий:

иметь высшее образование по направлению подготовки (специальности) в области математических и естественных наук, инженерного дела, технологий и технических наук;

пройти переподготовку по одной из специальностей направления подготовки «Информационная безопасность» в соответствии с Общероссийским классификатором специальностей (нормативный срок – не менее 360 часов);

стаж работы в сфере информационной безопасности не менее 3 лет.

6.3. Специалисты второй линии должны иметь высшее профессиональное образование по направлению подготовки «Информационная безопасность» в соответствии с Общероссийским классификатором специальностей или пройти переподготовку по одной из специальностей данного направления (нормативный срок – не менее 360 часов), а также стаж работы в сфере информационной безопасности не менее 3 лет.

6.4. Специалисты третьей линии должны иметь высшее профессиональное образование по направлению подготовки «Информационная безопасность» в соответствии с Общероссийским классификатором специальностей или пройти переподготовку по одной из специальностей данного направления (нормативный срок – не менее 360 часов), а также стаж работы в сфере информационной безопасности не менее 5 лет;

Специалисты всех линий должны проходить повышение квалификации не реже одного раза в 5 лет.

7. Взаимодействие Центра ГосСОПКА с НКЦКИ

7.1. Взаимодействие Центра ГосСОПКА с НКЦКИ осуществляется на основании:

соглашения о взаимодействии НКЦКИ и Правительства Самарской области в области обнаружения, предупреждения и ликвидации последствий компьютерных атак;

регламента взаимодействия НКЦКИ и Учреждения при информировании Федеральной службы безопасности Российской Федерации о компьютерных инцидентах, реагировании на компьютерные инциденты и принятии мер по ликвидации последствий компьютерных атак, совместно утверждаемого НКЦКИ и Центром ГосСОПКА;

иных документов, указанных в пункте 1.7 настоящего Положения.

ПРИЛОЖЕНИЕ 2
к приказу департамента
информационных технологий
и связи Самарской области
от 15.10.2021 № 93-п

Регламент
деятельности центра обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные системы и ресурсы Самарской области

Оглавление

Принятые аббревиатуры и сокращения 3
Принятые обозначения 3
1. Общие положения 8
2. Порядок функционирования 10
3. Организационная структура .....
4. Описание выполняемых Центром ГосСОПКА функций 11
4.1. Центр ГосСОПКА выполняет следующие функции: 12
4.2. Взаимодействие с НКЦКИ 13
4.3. Разработка документов, регламентирующих деятельность Центра ГосСОПКА 13
4.4. Эксплуатация средств, предназначенных для выполнения функций Центра ГосСОПКА 14
4.5. Прием сообщений о возможных инцидентах от персонала и пользователей ИР 15
4.6. Регистрация КА и КИ 16
4.7. Анализ событий ИБ 18
4.8. Инвентаризация ИР 18
4.9. Анализ угроз ИБ 20
4.10. Составление и актуализация перечня угроз ИБ для ИР 21
4.11. Выявление уязвимостей ИР 21
4.12. Формирование предложений по повышению уровня защищенности ИР 23
4.13. Составление перечня КИ 24
4.14. Ликвидация последствий КИ 30
4.15. Анализ результатов ликвидации последствий КИ 32
4.16. Установление причин КИ 33
5. Контактные данные для взаимодействия с НКЦКИ 34

Принятые аббревиатуры и сокращения

ВПО	вредоносное программное обеспечение
ГосСОПКА	государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
ИБ	информационная безопасность
ИР	информационный ресурс
КА	компьютерная атака
КИ	компьютерный инцидент
КИИ	критическая информационная инфраструктура
МГТС	межгородской телефонной сети
НКЦКИ	национальный координационный центр по компьютерным инцидентам
НСД	несанкционированный доступ
ОА	объект атаки
ОС	операционная система
ПО	программное обеспечение
ФСБ России	Федеральная служба безопасности Российской Федерации
ЦУ	центр управления

Принятые определения

ГосСОПКА	Единый централизованный, территориально распределенный комплекс, включающий силы и средства обнаружения, предупреждения и ликвидации последствий компьютерных атак и государственный орган, уполномоченный в области создания и обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
Зона ответственности	Совокупность информационных ресурсов, в отношении которых субъектом ГосСОПКА обеспечиваются обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирования на компьютерные инциденты.
Информационные ресурсы Российской Федерации	Информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, находящиеся на территории Российской Федерации и в дипломатических представительствах и (или) консульских учреждениях Российской Федерации

Компьютерная атака	Целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации
Компьютерный инцидент	Факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки
Критическая информационная инфраструктура	Объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов
Национальный координационный центр по компьютерным инцидентам	Организация, созданная ФСБ России, для обеспечения координации деятельности субъектов критической информационной инфраструктуры по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты (Главный Центр ГосСОПКА)
Субъекты ГосСОПКА	Государственные органы Российской Федерации, российские юридические лица и индивидуальные предприниматели, в силу закона или на основании заключенных с НКЦКИ соглашений осуществляющие обнаружение, предупреждение и ликвидацию последствий компьютерных атак и реагирование на компьютерные инциденты
Субъекты критической информационной инфраструктуры	Государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливноэнергетического комплекса, в области атомной энергии, оборонной, ракетно-космической,

	горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей
Центр (сегмент) ГосСОПКА	Структурная единица ГосСОПКА, представляющая совокупность подразделений и должностных лиц субъекта ГосСОПКА, которые принимают участие в обнаружении, предупреждении и ликвидации последствий компьютерных атак и реагировании на компьютерные инциденты в своей зоне ответственности: центр, созданный на базе государственного бюджетного учреждения Самарской области «Цифровой регион» (далее - Учреждение), находящегося в ведении департамента информационных технологий и связи Самарской области (далее – ДИТиС СО).
Информационная система	совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств (далее – ИС).
Доступ к информации	возможность получения информации и ее использования.
Средства обнаружения, предупреждения и ликвидации последствий компьютерных атак	технические, программные, лингвистические, правовые, организационные средства, включая сети и средства связи, средства сбора и анализа информации, поддержки принятия управленческих решений, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.
Обнаружение компьютерных атак	комплекс мероприятий по мониторингу и анализу функционирования информационных ресурсов с целью обнаружения компьютерных атак и компьютерных инцидентов.
Предупреждение компьютерных атак	комплекс превентивных мероприятий, направленных на снижение количества компьютерных инцидентов и повышение уровня защищенности информационных ресурсов.
Контроль (мониторинг) уровня(степени) защищенности информации в информационной системе	анализ и оценка функционирования системы защиты информации информационной системы, изменения угроз безопасности информации, защищенности информации, содержащейся в информационной системе.
Ликвидация последствий	комплекс мероприятий по восстановлению штатного режима функционирования информационных ресурсов

компьютерных атак	после компьютерных инцидентов.
Выявление уязвимостей	процесс выявления недостатков (включая уязвимости программного кода, ошибки в настройке, уязвимости архитектуры, ошибки в реализации мер защиты информации), которые могут использоваться нарушителем для проведения компьютерных атак.
Угроза безопасности информации	совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.
Анализ угроз	процесс определения возможных способов реализации угроз безопасности информации, включая определение возможных способов проведения компьютерных атак на информационную систему с учетом особенностей реализованных в ней информационных технологий, а также состава ее технических средств и программного обеспечения.
Событие информационной безопасности	идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной безопасности или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.
Корреляция событий информационной безопасности	взаимосвязь двух или более событий безопасности.
Нормализация событий безопасности	приведение сообщений о событиях безопасности к единому формату.
Реагирование на инцидент	совокупность действий, направленных на выявление компьютерной информации, имеющей отношение к инциденту, и сохранение ее целостности и юридической значимости, а также на сбор иных сведений, имеющих отношение к инциденту.
Установление причин компьютерных инцидентов	комплекс взаимосвязанных и согласованных по целям, задачам, месту и времени, силам и средствам мероприятий, направленных на установление технических причин и условий возникновения компьютерных инцидентов, а также ликвидацию последствий данных инцидентов.
Анализ инцидента (первичный)	комплекс мероприятий по обработке информации о компьютерном инциденте, проводимых с целью выявления причин и источников возникновения инцидента, особенностей его реализации, нанесенного им ущерба, использованных уязвимостей, а также другой доступной входящей информации об инциденте.
Комплексный анализ	исследование ряда выявленных компьютерных

инцидентов	инцидентов с целью выявления закономерностей их возникновения и динамики распространения, классификации и типизации, разработки моделей развития, подготовки прогнозов угроз информационной безопасности и для прочих задач, связанных с повышением эффективности стратегий предупреждения, обнаружения и установления причин компьютерных инцидентов, реагирования на них и ликвидации их последствий.
Инвентаризация информационного ресурса	деятельность, направленная на сбор информации об информационном ресурсе, в том числе о соответствующих объектах информатизации, включая используемое в них аппаратное и программное обеспечение.
Тестирование на проникновение	метод контроля уровня защищенности, основанный на выявлении и анализе известных или ранее не известных уязвимостей, которые могут использоваться для получения несанкционированного доступа к информационному ресурсу.
Тестирование устойчивости к атакам «отказ в обслуживании»	метод контроля уровня защищенности информационного ресурса, основанный на выявлении и анализе известных и ранее неизвестных уязвимостей, которые могут использоваться для нарушения доступности информационного ресурса.

1. Общие положения

1.1. Настоящий регламент разработан с целью определения порядка функционирования Центра ГосСОПКА в соответствии со следующими нормативными правовыми актами:

Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

Указ Президента Российской Федерации от 22.12.2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;

приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;

приказ ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»;

приказ ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них,

принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации»;

Требования к подразделениям и должностным лицам субъектов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, утвержденные директором НКЦКИ, от 26.04.2018 №149/2/7-322;

Положение о центре обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные системы и ресурсы Самарской области, утверждаемое приказом ДИТиС (далее - Положение о Центре ГосСОПКА);

иные нормативные правовые акты, а также внутренние нормативные документы, регламентирующие деятельность по созданию и развитию Центра ГосСОПКА.

2. Порядок функционирования

2.1. Задачи и функции, зона ответственности и требования к специалистам Центра ГосСОПКА определены в Положении о Центре ГосСОПКА.

2.2. Центр ГосСОПКА осуществляет взаимодействие с НКЦКИ в области обнаружения, предупреждения и ликвидации последствий компьютерных атак в соответствии со следующими нормативными документами, указанными в п.7.1 Положении о Центре ГосСОПКА.

3. Организационная структура

3.1. Центр ГосСОПКА создан на базе государственного бюджетного учреждения Самарской области «Цифровой регион» (далее- Учреждение), находящегося в ведении департамента информационных технологий и связи Самарской области (далее – ДИТиС СО).

Центр ГосСОПКА подчиняется директору Учреждения.

Руководство Центром ГосСОПКА осуществляет один из руководителей структурных подразделений Учреждения либо заместитель директора Учреждения на основании приказа директора Учреждения.

Специалисты Центра ГосСОПКА назначаются приказом руководителя Учреждения.

Структура и штатная численность Центра ГосСОПКА определяются приказом директора Учреждения.

Соответствие должностей Учреждения ролям Центра ГосСОПКА определяется в штатном расписании. Выполняемые специалистами функции указываются в должностных инструкциях сотрудников

4. Описание выполняемых Центром ГосСОПКА функций

4.1. Центр ГосСОПКА выполняет следующие функции:

1) взаимодействие с НКЦКИ при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы и реагирования на компьютерные инциденты, в том числе в части информационно-аналитического и прогностического обеспечения функционирования ГосСОПКА, предоставление в НКЦКИ сведений о состоянии защищенности информационных ресурсов от компьютерных атак и информации о компьютерных инцидентах в соответствии с установленным порядком;

2) разработка документов, регламентирующих процессы обнаружения, предупреждения и ликвидации последствий компьютерных инцидентов и реагирования на компьютерные инциденты;

3) эксплуатация средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, выявление ошибок в работе средств и направление производителю средств информации о выявленных ошибках, а также актуализация средств, используемых для обеспечения защиты информационных ресурсов, направление в НКЦКИ предложений по совершенствованию средств;

4) прием сообщений об инцидентах от персонала и пользователей информационных ресурсов;

5) регистрация компьютерных атак и компьютерных инцидентов;

6) анализ событий информационной безопасности;

7) инвентаризация информационных ресурсов;

8) анализ угроз информационной безопасности, прогнозирование их развития и направление в НКЦКИ результатов;

9) составление и актуализация перечня угроз информационной безопасности для информационных ресурсов;

10) выявление уязвимостей информационных ресурсов;

11) формирование предложений по повышению уровня защищенности информационных ресурсов;

12) составление перечня компьютерных инцидентов;

13) ликвидация последствий компьютерных инцидентов;

14) анализ результатов ликвидации последствий инцидентов;

15) установление причин компьютерных инцидентов.

4.2. Взаимодействие с НКЦКИ

4.2.1. Взаимодействие Центра ГосСОПКА с НКЦКИ осуществляется на основании соглашения о взаимодействии НКЦКИ и Правительства Самарской области в области обнаружения, предупреждения и ликвидации последствий компьютерных атак, Регламента взаимодействия Национального координационного центра по компьютерным инцидентам и государственного бюджетного учреждения Самарской области «Цифровой регион» при осуществлении информационного обмена в области обнаружения, предупреждения и ликвидации последствий компьютерных атак, совместно утверждаемого НКЦКИ и Центром ГосСОПКА, а также документов, указанных в пункте 1.7 Положения о Центре ГосСОПКА.

4.2.2 Взаимодействие осуществляется уполномоченными сотрудниками Центра ГосСОПКА.

4.3. Разработка документов, регламентирующих деятельность Центра ГосСОПКА

Деятельность всех структурных элементов сегмента ГосСОПКА подчиняется единой политике, устанавливаемой главным центром ГосСОПКА. При этом главный центр ГосСОПКА:

а) разрабатывает нормативные документы, определяющие порядок и особенности исполнения своих функций всеми структурными элементами сегмента ГосСОПКА;

б) определяет основные типы инцидентов, возможность возникновения которых поддается прогнозированию на основе имеющихся научно- технических возможностей сегмента ГосСОПКА (далее — типовые инциденты);

в) разрабатывает методические рекомендации по реализации комплекса мероприятий по обнаружению, предупреждению и ликвидации последствий типовых инцидентов, предназначенные для персонала сегмента ГосСОПКА и информационных ресурсов, находящихся в зоне его ответственности;

г) выполняет анализ результатов мероприятий по обнаружению, предупреждению и ликвидации последствий инцидентов и обеспечивает оценку их эффективности;

д) на основе анализа результатов указанных мероприятий уточняет (для типовых инцидентов) и разрабатывает (для инцидентов, не относившихся к типовым на момент возникновения) методические рекомендации по реализации комплекса мероприятий по обнаружению, предупреждению и ликвидации последствий инцидентов.

Зона ответственности Центра ГосСОПКА определяется в соответствии с Положением о Центре ГосСОПКА.

Основанием для включения информационных систем и ресурсов, оператором которых не является Учреждение, в зону ответственности Центра ГосСОПКА является передача права на обнаружение, предупреждение и ликвидацию последствий компьютерных атак на информационные ресурсы и реагирования на компьютерные инциденты на основании соглашений, договоров, государственных (муниципальных) контрактов.

4.4. Эксплуатация средств, предназначенных для выполнения функций Центра ГосСОПКА

Центр ГосСОПКА обеспечивает защиту информации, в соответствии с действующим законодательством Российской Федерации.

Аппаратные и программные средства, используемые для выполнения функций Центра ГосСОПКА:

средства антивирусной защиты;

замкнутая среда предварительного выполнения программ;

средство управления информацией об угрозах безопасности информации;

система контроля защищённости и соответствия стандартам;

система обеспечения мониторинга и корреляции инцидентов информационной безопасности;

средство обнаружения вторжений;

средство защиты информации среды виртуализации;

средство межсетевого экранирования;

система защиты приложений от несанкционированного доступа;

средство анализа исходного кода;

система анализа сетевого трафика.

4.5. Прием сообщений о возможных инцидентах от персонала и пользователей ИР

Центр ГосСОПКА обеспечивает централизованный прием сообщений о возможных компьютерных инцидентах с использованием средств взаимодействия с персоналом и пользователями информационных систем.

Центр ГосСОПКА принимает сообщения, сформулированные в произвольной форме, в том числе лицами, не обладающими необходимыми техническими знаниями. При наличии в сообщении неточностей, отсутствии необходимых сведений и при возможности диалога с автором сообщения специалисты Центра ГосСОПКА уточняют полученные сведения.

При приеме сообщений специалист Центра ГосСОПКА определяет следующий состав сведений об инциденте:

а) контактную информацию лица, сообщившего о компьютерном инциденте (если автор сообщения согласен предоставить такую информацию);

б) наименование информационных ресурсов, вовлеченных в компьютерный инцидент, а при невозможности такой идентификации — любые сведения, позволяющие прямо или косвенно определить такие ресурсы;

в) время обнаружения инцидента;

г) характер инцидента, как его понимает и может сформулировать автор сообщения;

д) сведения о принятых мерах, которыми располагает автор сообщения.

При получении сообщения специалист Центра ГосСОПКА проводит

регистрацию компьютерного инцидента в системе учета и обработки инцидентов путем создания карточки инцидента, в которую вносит все полученные сведения независимо от их полноты и достоверности.

4.6. Регистрация КА и КИ

Регистрация инцидентов осуществляется с использованием автоматизированных средств учета и обработки инцидентов.

При получении карточки инцидента специалист Центра ГосСОПКА проводит следующие мероприятия:

а) проверяет и уточняет сведения о возможном инциденте;

б) подтверждает факт возникновения инцидента и принимает решение о начале действий по реагированию на него;

в) определяет первоочередные меры реагирования на инцидент, определяет ответственных лиц и направляет им задания на реагирование.

В ходе проверки и уточнения сведений о возможном инциденте специалист Центра ГосСОПКА:

а) направляет лицам, ответственным за функционирование информационных ресурсов, предположительно затрагиваемых инцидентом, запрос на проверку сведений, содержащихся в карточке инцидента;

б) проводит самостоятельную проверку карточки инцидента путем сопоставления содержащихся в ней сведений с данными, полученными в процессе инвентаризации, выявления уязвимостей и анализа событий.

В случае если сведения о возможном инциденте подтверждаются специалистом Центра ГосСОПКА или хотя бы одним из лиц, ответственных за функционирование одного из информационных ресурсов, инцидент признается подтвержденным и принимаются меры реагирования. вплоть до приостановки функционирования информационной системы или ресурса.

Функционирование информационной системы или ресурса приостанавливается в качестве экстренной меры реагирования с последующим оповещением его владельца в следующих случаях:

дальнейшая его эксплуатация является угрозой информационной безопасности для других информационных систем или ресурсов;

дальнейшая его эксплуатация может повлечь распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность;

дальнейшая его эксплуатация может повлечь распространения угрозы, компьютерной атаки, вредоносной активности;

на информационном ресурсе обнаружен факт использования вычислительных ресурсов для майнинга.

Факт приостановки информационной системы или ресурса фиксируется в отчете об инциденте, направляемом владельцу информационного ресурса.

Целью обнаружения компьютерных атак является своевременное реагирование на связанные с ними инциденты, принятие мер по ликвидации последствий таких инцидентов.

В ходе деятельности по обнаружению компьютерных атак реализуются следующие процессы:

а) контроля за реализацией правил эксплуатации средств обнаружения компьютерных атак на информационные ресурсы;

б) контроля за централизованным обновлением баз решающих правил для средств обнаружения компьютерных атак Центра ГосСОПКА;

в) выявления ранее неизвестных компьютерных атак сетевого уровня, в том числе с применением средств анализа сетевого трафика на каналах связи;

г) выявления ранее неизвестных компьютерных атак, проводимых с использованием вредоносного программного обеспечения, в том числе с использованием методов поведенческого анализа программного обеспечения;

д) разработки решающих правил для неизвестных компьютерных атак.

При обнаружении ранее неизвестных компьютерных атак Центром ГосСОПКА проводятся мероприятия по реализации функции анализа угроз информационной безопасности, представленные в пункте 4.9 настоящего Регламента.

4.7. Анализ событий ИБ

Целью анализа событий информационной безопасности является регистрация инцидентов, в том числе связанных с ранее неизвестными компьютерными атаками, а также инцидентов, связанных с недостаточной эффективностью принимаемых мер защиты информации. Обработка (сбор, анализ и хранение) данных о событиях информационной безопасности производится Центром ГосСОПКА в зоне его ответственности.

Для реализации анализа событий информационной безопасности Центр ГосСОПКА осуществляет сбор результатов работы всех средств защиты информации, используемых в соответствии с политикой безопасности, принятой в информационных системах.

Источниками информации об инцидентах информационной безопасности в том числе являются:

факты, выявленные сотрудниками органов и организаций, чьи ресурсы включены в зону ответственности Центра Госсопка;

результаты работы средств мониторинга информационной безопасности, аудита (внутреннего или внешнего);

журналы и оповещения операционных систем серверов и рабочих станций, антивирусной системы, системы резервного копирования и других систем;

обращения субъектов персональных данных с указанием инцидента информационной безопасности;

сообщения Федеральной службы технического и экспортного контроля России (далее – ФСТЭК России);

сообщения ФСБ России;

сообщения Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций.

4.8. Инвентаризация ИР

Целью инвентаризации является получение и поддержание в актуальном

состоянии сведений об информационных ресурсах, необходимых для выполнения функций Центра ГосСОПКА.

Деятельность по инвентаризации включает в себя следующие этапы сбора сведений об информационном ресурсе:

а) фамилии, имена и отчества, должности и контактные данные лиц, ответственных за функционирование информационного ресурса;

б) доменные имена и сетевые адреса компонентов информационного ресурса (средств вычислительной техники, телекоммуникационного оборудования, виртуальных машин и т.д.) в соответствии с системой имен и сетевой адресацией информационного ресурса;

в) доменные имена и сетевые адреса компонентов информационного ресурса, доступные из сети Интернет, в соответствии с системой имен и сетевой адресацией сети Интернет, а также сведения о протоколах (включая параметры транспортного уровня взаимодействия), по которым разрешен доступ к этим компонентам;

г) сведения о сегментации и топологии локальных вычислительных сетей, правилах маршрутизации и коммутации, настройках средств межсетевого экранирования;

д) перечень программного обеспечения (прикладного и системного), установленного на каждом средстве вычислительной техники;

е) параметры настройки программного и аппаратного обеспечения информационного ресурса, существенные с точки зрения обеспечения безопасности информации;

ж) параметры настройки средств обеспечения информационной безопасности.

Инвентаризация информационных ресурсов проводится:

не реже одного раза в год;

для всех компонентов информационных ресурсов, находящихся в зоне ответственности Центра ГосСОПКА (включая средства вычислительной техники, принадлежащие иным организациям, подключенные временно, предоставленные для тестирования и т. п.);

при каждом изменении состава программного и (или) аппаратного обеспечения средств вычислительной техники, телекоммуникационного

оборудования и виртуальных машин (путем ежедневного или событийного контроля изменений, а также иными способами, обеспечивающими уточнение инвентаризационной информации в течение пяти рабочих дней со дня внесения изменений).

Сбор инвентаризационной информации выполняется Центром ГосСОПКА в пределах его зоны ответственности.

4.9. Анализ угроз ИБ

Целью анализа угроз информационной безопасности является определение возможных способов проведения компьютерных атак на информационную систему с учетом особенностей реализованных в ней информационных технологий, состава ее технических средств и программного обеспечения, а также разработка предложений по противодействию компьютерным атакам, представляющим угрозу соответствующим информационным ресурсам.

Анализ угроз проводится на основе инвентаризационной информации и результатов выявления уязвимостей и включает в себя:

а) определение возможных угроз, связанных с компьютерными атаками на данный информационный ресурс;

б) идентификацию уязвимостей, использование которых может позволить нарушителю выполнить такие атаки;

в) определение способов проведения компьютерных атак с использованием таких уязвимостей;

г) определение возможных признаков проведения таких компьютерных атак, способов их обнаружения и мер реагирования на них;

д) определение возможных путей противодействия проведению таких компьютерных атак;

е) выработку организационных и технических решений по противодействию компьютерным атакам.

На основе анализа угроз разрабатываются новые или уточняются существующие документы.

4.10. Составление и актуализация перечня угроз ИБ для ИР

В рамках взаимодействия между НКЦКИ и Центром ГосСОПКА возможен обмен информацией об актуальных угрозах информационной безопасности с предоставлением следующей информации:

а) тип угрозы;

б) источник получения информации об угрозе;

в) направленность угрозы информационной безопасности;

г) описание угрозы информационной безопасности;

д) время получения информации об угрозе информационной безопасности;

е) запрос на оказание помощи и (или) выполнение мероприятий по нейтрализации угроз информационной безопасности.

4.11. Выявление уязвимостей ИР

Целью выявления уязвимостей является определение недостатков в обеспечении безопасности информационных ресурсов (включая уязвимости программного кода, ошибки в настойке, уязвимости архитектуры, ошибки в реализации мер защиты), которые могут использоваться нарушителем для проведения компьютерных атак. Выявление уязвимостей включает в себя оценку степени их опасности и разработку рекомендаций по их устранению.

Выявление уязвимостей выполняется следующими способами:

а) выявление известных уязвимостей сетевых служб, доступных для сетевого взаимодействия, с применением автоматизированных средств анализа защищенности (сетевое сканирование);

б) выявление известных уязвимостей программного обеспечения информационных ресурсов путем анализа состава установленного программного обеспечения и обновлений безопасности с применением автоматизированных средств анализа защищенности (системное сканирование, исследование с использованием привилегированных учетных записей и (или) программных агентов), а также других средств защиты информации;

в) тестирование на проникновение в условиях, соответствующих условиям

нарушителя, действующего со стороны сети Интернет и (или) со стороны информационных ресурсов, внешних по отношению к зоне ответственности Центра ГосСОПКА;

г) тестирование на проникновение в условиях, соответствующих условиям нарушителя, действующего со стороны информационных ресурсов, входящих в зону ответственности Центра ГосСОПКА;

д) тестирование устойчивости к атакам типа «отказ в обслуживании»;

е) контроль устранения ранее выявленных уязвимостей и недостатков;

ж) контроль выполнения требований безопасности информации, предъявляемых к контролируемой информационной системе;

з) анализ настроек программного и аппаратного обеспечения информационных систем, а также средств защиты информации;

и) анализ проектной, конструкторской и эксплуатационной документации информационных систем;

к) оценка соответствия применяемых мер защиты требованиям безопасности информации, предъявляемым к информационным ресурсам нормативными документами Российской Федерации и владельцев информационных ресурсов;

л) анализ исходного кода.

В случаях, определенных нормативными документами Российской Федерации, для выявления уязвимостей применяется статический и динамический анализ исходного кода программного обеспечения информационных ресурсов (для программного обеспечения, поставляемого с исходными кодами).

Выявление уязвимостей проводится для каждого информационного ресурса со следующей периодичностью:

а) сетевое и системное сканирование, анализ настроек - не реже одного раза в квартал;

б) тестирование на проникновение и тестирование устойчивости к атакам типа «отказ в обслуживании» - не реже одного раза в год;

в) контроль выполнения требований безопасности информации — не реже одного раза в квартал;

г) контроль устранения ранее выявленных уязвимостей и недостатков –

не реже одного раза в квартал;

д) оценка соответствия применяемых мер защиты требованиям безопасности информации, предъявляемым к информационным ресурсам нормативными документами Российской Федерации и владельцев информационных ресурсов – не реже одного раза в два года;

е) анализ проектной, конструкторской и эксплуатационной документации – перед вводом информационного ресурса в эксплуатацию и при каждом изменении состава программных или аппаратных средств;

ж) анализ исходного кода – перед вводом информационного ресурса в эксплуатацию и при каждом изменении программного обеспечения, поставляемого с исходным кодом.

Центр ГосСОПКА предоставляет актуальную информацию о выявленных уязвимостях главному центру ГосСОПКА путем отправки в главный центр ГосСОПКА отчетов с результатами всех проводимых мероприятий по данному направлению деятельности.

4.12. Формирование предложений по повышению уровня защищенности ИР

По результатам обнаружения КА разрабатываются рекомендации по повышению уровня защищенности ОА, в которых необходимо выделять первоочередные меры, требующие реализации в максимально сжатые сроки.

В качестве типовых рекомендаций по повышению уровня защищенности ОА используются следующие рекомендации по повышению уровня защищенности ОА от КА, направленных на получение НСД к ОА:

В целях минимизации возможностей атакующего по успешной реализации КА, направленных на получение НСД к ОА, рекомендуется:

1. Отключить на ОА неиспользуемые для удаленного управления им сетевые сервисы.

2. С использованием средств межсетевого экранирования ограничить возможность удаленного подключения к ОА.

3. Использовать только стойкие к перебору пароли с ограничением срока их действия, а также количества одновременных попыток их ввода или времени между

ними.

4. Принять меры по устранению использованных атакующим уязвимостей путем настройки и обновления системного и ППО ОА, включая средства защиты информации.

Рекомендации по повышению уровня защищенности ОА от КА, направленных на блокирование доступности ОА:

В целях минимизации возможностей атакующего по успешной реализации КА, направленных на блокирование доступности ОА, рекомендуется следующее:

1. Организовать мониторинг доступности ОА.

2. Установить ограничение на «время жизни» неактивных сессий.

3. Предусмотреть возможность оперативного переключения ОА на резервный канал связи с переназначением IP-адреса ОА.

4. Организовать взаимодействие с Интернет-провайдерами и другими организациями по вопросам использования услуг по защите от КА, направленных на блокирование доступности ОА.

5. Организовать распределение обращений к ОА с использованием балансировщиков нагрузки.

6. Использовать технологию CDN.

7. Использовать технологии ограничения пропускной способности канала доступа в сеть Интернет для ОА.

4.13. Составление перечня КИ

Для взаимодействия по вопросам обмена информацией о компьютерных инцидентах (КИ) используется следующая карточка компьютерного инцидента.

Общие поля:

1. Идентификатор инцидента (порядковый номер инцидента). Поле заполняется уникальным буквенно-числовым значением длиной не более 15 символов. Установленный формат идентификатора компьютерного инцидента не может быть изменен с течением времени.

2. TLP. Поле предназначено для маркировки конфиденциальной информации с целью указания аудитории ее дальнейшего распространения.

Заполняется исходя из степени конфиденциальности передаваемой информации. Используются маркировки следующего типа:

Red (Красный). Ознакомление с информацией ограничивается исключительно лицом, указанным в качестве адресата. Ознакомление с материалами с данной пометкой также возможно для руководителей участвующих сторон обмена и специалистов, в чьи полномочия входит решение вопросов соответствующей тематики сообщения без права передачи третьим лицам и сторонним организациям.

Amber (Желтый). Ознакомление с информацией ограничивается кругом специалистов участвующих сторон, работников, имеющих легитимный доступ к защищаемому информационному ресурсу, сотрудников правоохранительных органов и специалистов сторонних организаций, привлекаемых к обеспечению защиты информации данного информационного ресурса. При передаче такой информации указанным лицам в сопроводительном тексте для них делается запись о недопустимости распространения направляемых сведений.

Green (Зеленый). Возможна передача информации для ознакомления специалистам в сфере информационной безопасности и другим лицам. При распространении такой информации сохраняется авторство первоисточника.

3. Статус инцидента. Возможны следующие статусы:

меры приняты, инцидент исчерпан (вес — 0);

меры приняты, инцидент не исчерпан (вес —10).

Поле предназначено для указания состояния КИ. КИ является исчерпанным в случае, если вредоносные воздействия завершились и были приняты меры по предотвращению последствий компьютерного инцидента.

4. Необходимость содействия. Значение поля может быть:

необходимо содействие (вес — 10);

нет необходимости в содействии (вес — 0).

Какой именно тип содействия необходим, указывается в поле комментария в карточке КИ. Существуют следующие типы содействия со стороны НКЦКИ:

передача информации об IP-адресах и доменных именах, осуществляющих вредоносные воздействия, уполномоченным организациям в различных странах мира для принятия мер по предотвращению вредоносной деятельности на ресурсы

Российской Федерации;

прекращение вредоносной активности IP-адресов и доменных имен, находящихся в адресном пространстве Российской Федерации;

получение дополнительной информации об участниках КИ из специализированных источников и баз знаний НКЦКИ;

анализ образцов вредоносного программного обеспечения для последующего выявления управляющих серверов и анализа его жизненного цикла;

анализ журналов, образов ОС и другой информации, полученной в рамках реагирования на компьютерные инциденты, с целью получения полной информации о КИ;

анализ КИ на связи с другими инцидентами;

консультации по предотвращению последствий КИ;

координация деятельности заинтересованных сторон по ликвидации КИ и предотвращению их последствий;

мероприятия по оценки защищенности.

5. Тип инцидента (один инцидент может иметь комбинированный тип):

Группа 1 (вес — 4):

ВПО (включая APT и бот-агент);

несанкционированный доступ;

эксплуатация уязвимости;

Группа 2 (вес — 3):

DoS/DDoS;

перебор паролей;

ЦУ бот-сети;

Группа 3 (вес — 2):

фишинг (мошенничество);

вредоносный ресурс;

запрещенный контент (нарушение прав);

Группа 4 (вес — 1):

сканирование ресурсов;

спам;

нарушение политики безопасности;

другое (вес — 0).

6. Опасность инцидента:

Рассчитывается по формуле: вес статуса + вес содействия + вес типа инцидента.

7. Дата и время фиксирования инцидента (UTC+0).

8. Дата и время создания карточки инцидента (UTC+0).

9. Источник поступления информации об инциденте (если возможно указать; департамент, управление, отдел, средства, которыми был выявлен инцидент и т. п.).

10. Описание инцидента и комментарии (включая хронологию принятых мер).

11. Связь с другими инцидентами (по номеру идентификатора).

12. Контакты:

контактное лицо, ответственное по данному инциденту (фамилия, имя, отчество (в случае наличия), номер МГТС, электронная почта);

контакты пострадавшей стороны (в случае наличия);

контакты возможного злоумышленника (в случае наличия);

контакты технического специалиста на объекте (в случае наличия).

13. Описание полей карточки инцидента, специфичной по типу инцидента (набор полей может изменяться в зависимости от ситуации, подтипа инцидента или полноты известной информации по инциденту).

А. DoS/DDos:

IP-адрес пострадавшей стороны;

IP-адреса атакующих;

тип атаки (если возможно определить);

мощность атаки (если возможно определить; пакетов в секунду, байтов в секунду).

Б. Перебор паролей:

IP-адрес пострадавшей стороны;

IP-адреса атакующих;

тип протокола;

- мощность атаки (если возможно определить; пакетов в секунду,

байтов в секунду).

В. Сканирование ресурсов:

IP-адрес пострадавшей стороны;

IP-адрес атакующего;

список сканируемых портов;

методы сканирования или ПО (если возможно определить).

Г. Спам:

IP-адрес пострадавшей стороны;

IP-адреса атакующих;

количество почтовых сообщений (если возможно определить).

Д. Фишинг (мошенничество):

IP-адрес пострадавшей стороны;

IP-адрес (URL) вредоносного ресурса;

IP-адрес (URL) легитимного ресурса;

программное обеспечение, используемое в мошеннических целях;

адреса электронной почты, с которых поступило письмо с вложением;

образец ВПО (если возможно получить);

тип ВПО, хеш, идентификатор ВПО (если возможно определить);

исходный код электронного письма или EML.

Е. Вредоносный ресурс:

тип вредоносного ресурса (если возможно определить);

IP-адрес пострадавшей стороны;

IP-адрес (URL) вредоносного ресурса;

тип ВПО, хеш, идентификатор ВПО с указанием лаборатории (при обнаружении, если возможно определить);

образец ВПО (если возможно получить);

эксплуатируемая CVE.

Ж. ВПО:

IP-адрес бот-агента;

тип и общие сведения о бот-сети (если возможно определить);

ЦУ, доменное имя и IP-адрес (если возможно определить);

тип ВПО, хеш, идентификатор ВПО (если возможно определить);

образец ВПО (если возможно получить).

З. ЦУ бот-сети:

IP-адрес и доменное имя ЦУ;

тип и общие сведения о бот-сети;

способ выявления.

И. Эксплуатация уязвимостей:

задействованные IP-адреса;

класс уязвимости;

последствия эксплуатации уязвимости.

К. Несанкционированный доступ:

IP-адрес пострадавшей стороны;

IP-адрес атакующего;

способ получения НСД, протокол (если возможно определить);

последствия несанкционированного доступа.

Л. Запрещенный контент:

IP-адрес и доменное имя пострадавшей стороны;

IP-адрес атакующего;

тип контента;

причина размещения контента.

М. Нарушение политики безопасности (полное описание инцидента и вся дополнительная информация).

Н. Другое (полное описание инцидента и вся дополнительная информация).

При передаче информации о компьютерном инциденте в автоматическом режиме карточка инцидента передается в формате JSON или XML. Формат согласуется на этапе организации взаимодействия с каждым сегментом ГосСОПКА индивидуально.

Центр ГосСОПКА обеспечивает хранение всех событий безопасности, журналов прикладного программного обеспечения и другой информации, полученных в рамках компьютерного инцидента на срок не менее 6 (шести) месяцев.

Вне очереди направляются инциденты:

с запросом содействия;

по которым были приняты меры, но инцидент не исчерпан;

инциденты группы 1 и группы 2.

Остальные компьютерные инциденты направляются при их локализации (статус: меры приняты, инцидент исчерпан).

4.14. Ликвидация последствий КИ

Реагирование на инцидент включает в себя:

а) фиксацию состояния и анализ объектов информационных ресурсов, вовлеченных в инцидент;

б) координацию деятельности по прекращению воздействия компьютерных атак, проведение которых вызвало возникновение инцидента;

в) фиксацию и анализ сетевого трафика, циркулирующего в информационном ресурсе, вовлеченном в инцидент;

г) определение причин инцидента и возможных его последствий для информационного ресурса;

д) локализацию инцидента;

е) сбор сведений для последующего установления причин инцидента;

ж) планирование мер по ликвидации последствий инцидента;

з) ликвидацию последствий инцидента;

и) контроль ликвидации последствий;

к) формирование рекомендаций для совершенствования нормативных документов, в соответствии с которыми осуществляется деятельность Центра ГосСОПКА и специалистов, обеспечивающих информационную безопасность информационных ресурсов.

Определение причин инцидента проводится специалистом Центра ГосСОПКА совместно с персоналом информационной системы и (или) информационного ресурса. При этом:

а) специалист Центра ГосСОПКА оперирует данными инвентаризации, выявления уязвимостей и анализа событий безопасности, а также направляет лицу,

ответственному за функционирование информационного ресурса, запросы на предоставление дополнительных сведений;

б) персонал информационного ресурса действует в пределах своей компетенции в соответствии с инструкциями, а также в соответствии с указаниями специалиста центра ГосСОПКА.

В случае, если запрос специалиста Центра ГосСОПКА предполагает выполнение действий, не предусмотренных эксплуатационной документацией информационного ресурса и способных привести к нарушению его функционирования, решение о допустимости выполнения запроса принимает лицо, ответственное за функционирование информационного ресурса с учетом обстоятельств инцидента.

Лицо, ответственное за функционирование информационного ресурса, совместно со специалистами Центра ГосСОПКА организует локализацию инцидента и ликвидацию последствий в соответствии с рекомендациями, разработанными для инцидентов данного типа.

Координация действий по реагированию на инцидент возлагается на специалиста Центра ГосСОПКА. Специалист Центра ГосСОПКА, формирует рабочую группу, состоящую из специалистов, ответственных за функционирование затронутых инцидентом информационных ресурсов. Рабочая группа принимает решение о мерах по локализации инцидента.

Решения принимаются рабочей группой отдельно для каждого информационного ресурса, затронутого инцидентом. Каждое решение утверждается лицом, ответственным за функционирование информационного ресурса, по согласованию со специалистом Центра ГосСОПКА, координирующим действия по реагированию на инцидент. Решения, затрагивающие функционирование прочих информационных ресурсов, принимаются по согласованию с лицами, ответственными за их функционирование.

Решения о ликвидации последствий инцидента принимаются в аналогичном порядке по результатам установления причин инцидента.

4.15. Анализ результатов ликвидации последствий КИ

Инцидент признается завершенным после принятия всех мер, предусмотренных методическими рекомендациями и (или) решением рабочей группы, при условии, что установление причин инцидента показало достаточность принятых мер.

Анализ результатов устранения последствий инцидента включает в себя оценку:

а) вреда, причиненного информационному ресурсу и его владельцу в результате инцидента;

б) недостатков в обеспечении безопасности информации, не позволивших предотвратить инцидент;

в) своевременности обнаружения инцидента;

г) действий персонала при локализации инцидента и ликвидации его последствий;

д) сроков устранения последствий инцидента.

При оценке вреда, причиненного информационному ресурсу и его владельцу в результате инцидента, учитываются:

а) трудозатраты персонала и иные затраты, связанные с ликвидацией последствий;

б) вред, причиненный общественным интересам и интересам владельца информационного ресурса, в том числе связанный с нарушением конфиденциальности, целостности и доступности сведений, обрабатываемых затронутыми информационными ресурсами.

При оценке недостатков в обеспечении безопасности информации определяются:

а) нормативные требования, невыполнение, недостаточная эффективность выполнения или отсутствие которых сделали инцидент возможным;

б) дополнительные меры защиты, которые не являются обязательными в соответствии с действующими нормативными документами, но которые могли бы предотвратить инцидент.

На основании оценки вреда и недостатков разрабатываются рекомендации по

предупреждению подобных инцидентов и стандартный порядок действий при их повторении.

При оценке своевременности обнаружения инцидента принимаются в расчет:

а) сведения об инциденте, выявленные в ходе установления его причин, на основании которых можно судить о времени фактического начала компьютерной атаки, которая привела к инциденту;

б) время, прошедшее с фактического начала компьютерной атаки до регистрации инцидента.

Решение о своевременности обнаружения инцидента принимается лицами, ответственными за функционирование информационных ресурсов, затронутых инцидентом. В случае если обнаружение инцидента признается несвоевременным хотя бы для одного из затронутых информационных ресурсов, разрабатываются предложения по совершенствованию применяемых технических средств и процедур обнаружения, предупреждения и ликвидации последствий компьютерных атак.

По результатам анализа инцидента, связанного с ранее неизвестной компьютерной атакой, Центр ГосСОПКА осуществляет самостоятельную разработку или уточнение существующих методических рекомендаций по обнаружению, предупреждению и ликвидации последствий компьютерных атак данного типа.

4.16. Установление причин КИ

Установление причин инцидента проводится в две стадии:

а) первичный анализ инцидента;

б) комплексный анализ инцидента.

Задачами первичного анализа инцидента являются:

а) установление обстоятельств и возможных последствий инцидента;

б) установление обстоятельств инцидента, выходящих за рамки стандартного порядка действий при инциденте данного типа.

Задачами комплексного анализа инцидента являются:

а) установление причин инцидента;

б) установление фактических последствий инцидента.

Первичный анализ инцидента проводится одновременно с локализацией инцидента Центром ГосСОПКА. Одновременно с ликвидацией последствий инцидента Центром ГосСОПКА совместно с главным Центром ГосСОПКА и оператором информационной системы и (или) информационного ресурса проводится комплексный анализ инцидента.

На обеих стадиях осуществляется сбор сведений об инциденте и их анализ.

В ходе анализа сведений делаются выводы об обстоятельствах инцидента, характере атаки, а также возможных путях развития инцидента и его последствиях, рассматривается вопрос о необходимости передачи информации об инциденте в правоохранительные органы для проведения расследования. Сведения об инциденте сохраняются для последующей разработки или уточнения методических рекомендаций по обнаружению, предупреждению и ликвидации последствий аналогичных инцидентов. Сбор и анализ сведений проводятся на протяжении всего комплекса мероприятий по ликвидации последствий инцидента.

5. Контактные данные для взаимодействия с НКЦКИ

5.1. Со стороны ГБУ СО «Цифровой регион»:

Сетевой адрес автоматизированного рабочего места в сети Интернет: 194.110.10.220;

Адрес электронной почты: isc@digitalreg.ru;

Контактный телефон: 8 (846) 200-09-39;

Почтовый адрес – isc@digitalreg.ru

Руководитель Центра ГосСОПКА – заместитель директора Акимов Максим Олегович.

Руководитель ГБУ СО «Цифровой регион» – директор Денисов Александр Михайлович.

5.2. Со стороны НКЦКИ:

Сетевой адрес портала НКЦКИ в сети Интернет: cert.gov.ru;

Номер сети для защищённого подключения: 10976;

Адрес портала НКЦКИ: portal.cert.local;

Адрес электронной почты для обмена информацией касательно компьютерных инцидентов: incident@cert.gov.ru;

Адрес электронной почты для взаимодействия по остальным вопросам: info@cert.gov.ru;

Почтовый адрес: 107031, г. Москва, ул. Большая Лубянка, д. 1/3;

Контактные телефоны: 8 (916) 901-07-42, 8(499) 196-75-91.