«Основы кибербезопасности»

Общие вопросы обеспечения кибербезопасности

План лекции

УЧЕБНЫЕ ВОПРОСЫ :

1. Понятие кибербезопасности.

2. Методы совершения киберпреступлений.

3. Уязвимости интернета вещей.

План лекции

УЧЕБНЫЕ ВОПРОСЫ :

4. Центры мониторинга и управления безопасностью.

5. Понятие Критической информационной инфраструктуры.

ЛИТЕРАТУРА

Нормативно-правовые акты, официальные издания

1. Об информации, информационных технологиях и защите информации : федеральный закон от 27.07.2006 №149-ФЗ.
2. Уголовный кодекс Российской Федерации : федеральный закон от 13.06.1996 №63-ФЗ.
3. Кодекс Российской Федерации об административных правонарушениях : федеральный закон от 30.12.2001 №195-ФЗ.

ЛИТЕРАТУРА

Нормативно-правовые акты, официальные издания

4. О полиции : федеральный закон от 07.02.2011 №3-ФЗ.
5. О персональных данных : федеральный закон от 27.07.2006 №152-ФЗ.
6. Защита информации. Основные термины и определения: ГОСТ Р 50922-2006. – Введ. 2006-12-27.
7. Защита информации. Система стандартов. Основные положения : ГОСТ Р 52069.0-2013. - Введ. 2013-02-28.

ЛИТЕРАТУРА

Основная литература

1. Основы информационной безопасности в органах внутренних дел [Электронный ресурс] : учеб. пособие / сост. А.Б. Сизоненко, С. Г. Клюев, В. Н. Цимбал. - Краснодар : Краснодар. ун-т МВД России, 2016. - 122 с.

2. Основы информационной безопасности : учебник / [В. Ю. Рогозин и др.]. - Москва : ЮНИТИ- ДАНА, 2016. - 287 с.

ЛИТЕРАТУРА

Основная литература

3. Основы информационной безопасности в органах внутренних дел [Электронный ресурс] : учеб. пособие / К. Л. Костюченко, С. В. Мухачев. - Екатеринбург : УрЮИ МВД России, 2015. - 155с.

4. Цымбаленко С.В. Основы информационной безопасности в органах внутренних дел [Электронный ресурс] : учеб. пособие / С.В. Цымбаленко. – Ставрополь: СФ КрУ МВД России, 2017. 140 с.

1. Понятие кибербезопасности

«Концепция стратегии кибербезопасности Российской Федерации» 10.01.2014 года не была принята из-за позиции ФСБ России.

Международный стандарт ИСО/МЭК 27032:2012 Руководящие указания по кибербезопасности «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по кибербезопасности»

(ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity)

Информационное пространство **– сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию**

Информационная безопасность **– состояние защищенности личности, организации и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве.**

Киберпространство **– сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства).**

Кибербезопасность **– совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями.**

Киберпространство **– комплексная виртуальная среда (не имеющая физического воплощения), сформированная в результате действий людей, программ и сервисов в сети Интернет посредством соответствующих сетевых и коммуникационных технологий.**

Кибербезопасность **– свойство защищенности активов от угроз конфиденциальности, целостности, доступности в киберпространстве.**

Кибербезопасность **– свойство защищенности активов от угроз конфиденциальности, целостности, доступности в киберпространстве.**

Кибербезопасность *– это деятельность, направленная на защиту систем, сетей и программ от цифровых атак.*

Кибербезопасность *(компьютерная безопасность) – это совокупность методов и практик защиты от атак злоумышленников на компьютеры, серверы, мобильные устройства , электронные системы, сети и данные.*

Киберпространство **– это сложная среда, создаваемая совокупностью информации, информационной среды и информационного взаимодействия субъектов с использованием информации получаемой (передаваемой) и обрабатываемой в информационной среде.**

Кибербезопасность **– это состояние защищенности киберпространства.**

Киберугроза **– это совокупность условий и факторов, создающих потенциальную или реально существующую опасность причинения вреда киберпространству.**

Киберпреступность **– преступная деятельность, в которой техническая инфраструктура киберпространства используется в целях совершения преступления или является целью преступления, или где киберпространство является источником, инструментом, целью или местом преступления.**

Объекты атак

- Инфраструктура
- Веб-ресурсы
- Пользователи
- Банкоматы и POS-терминалы
- Мобильные устройства
- IoT

Методы атак

- Использование вредоносного ПО
- Подбор учетных данных
- Социальная инженерия
- Хакинг
- Эксплуатация веб-уязвимостей

Категории жертв

- Финансовая отрасль
- Государственные учреждения
- Медицинские учреждения
- Наука и образование
- Промышленные компании
- Оборонные предприятия
- Онлайн-сервисы
- Сфера услуг
- Транспорт
- IT-компании
- Торговля
- Частные лица
- Телекоммуникационные компании
- Блокчейн-проекты
- Другие сферы

2. Методы совершения киберпреступлений

Киберпреступления **– все преступления, в которых компьютер, информационно-телекоммуникационные технологии или сети выступают предметом, средством или орудием преступления.**

Виды киберпреступлений:

1.Против компьютерных данных и систем.

2. С использованием компьютерных средств.

3. Связаны с контентом.

4. Нарушение авторских и смежных прав.

5. Кибертерроризм

Особенности киберпреступлений:

1. Повышенная скрытность совершения.

2. Трансграничные характер.

3. Особая подготовленность преступников, интеллектуальный характер преступной деятельности.

4. Возможность совершения преступления в автоматизированном режиме в нескольких местах одновременно.

Особенности киберпреступлений:

5. Неосведомленность потерпевших о том, то они подверглись преступному воздействию.

6. Дистанционный характер преступных действий в условиях отсутствия физического контакта преступника и потерпевшего.

7. Невозможность предотвращения и пресечения преступлений данного вида традиционными средствами.

Программное обеспечение, которое наносит вред, – самый распространенный инструмент киберпреступников. Они создают его сами, чтобы с его помощью повредить компьютер пользователя и данные на нем или вывести его из строя. Вредоносное ПО часто распространяется под видом безобидных файлов или почтовых вложений.

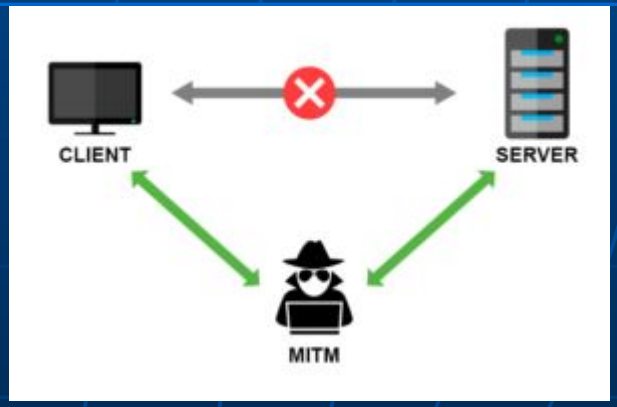
Виды вредоносного программного обеспечения:

- ***вирусы;***
- ***троянские программы;***
- ***сетевые черви;***
- ***шпионское ПО;***
- ***программы-вымогатели;***
- ***рекламное ПО.***

SQL-инъекция - этот вид кибератак используется для кражи информации из баз данных. Киберпреступники используют уязвимости в приложениях, управляющих данными, чтобы распространить вредоносный код на языке управления базами данных (SQL).

Фишинг – атаки, цель которых – обманом заполучить конфиденциальную информацию пользователя (например, данные банковских карт или пароли).

Атаки Man-in-the-Middle («человек посередине») - это атака, в ходе которой киберпреступник перехватывает данные во время их передачи – он как бы становится промежуточным звеном в цепи, и жертвы об этом даже не подозревают.



DoS-атаки (атаки типа «отказ в обслуживании») - киберпреступники создают избыточную нагрузку на сети и серверы объекта атаки, из-за чего система прекращает нормально работать и ею становится невозможно пользоваться.

Как защититься от атак:

- *обновите программное обеспечение и операционную систему;*
- *используйте антивирусные программы;*
- *используйте надежные пароли;*
- *не открывайте почтовые вложения от неизвестных отправителей;*

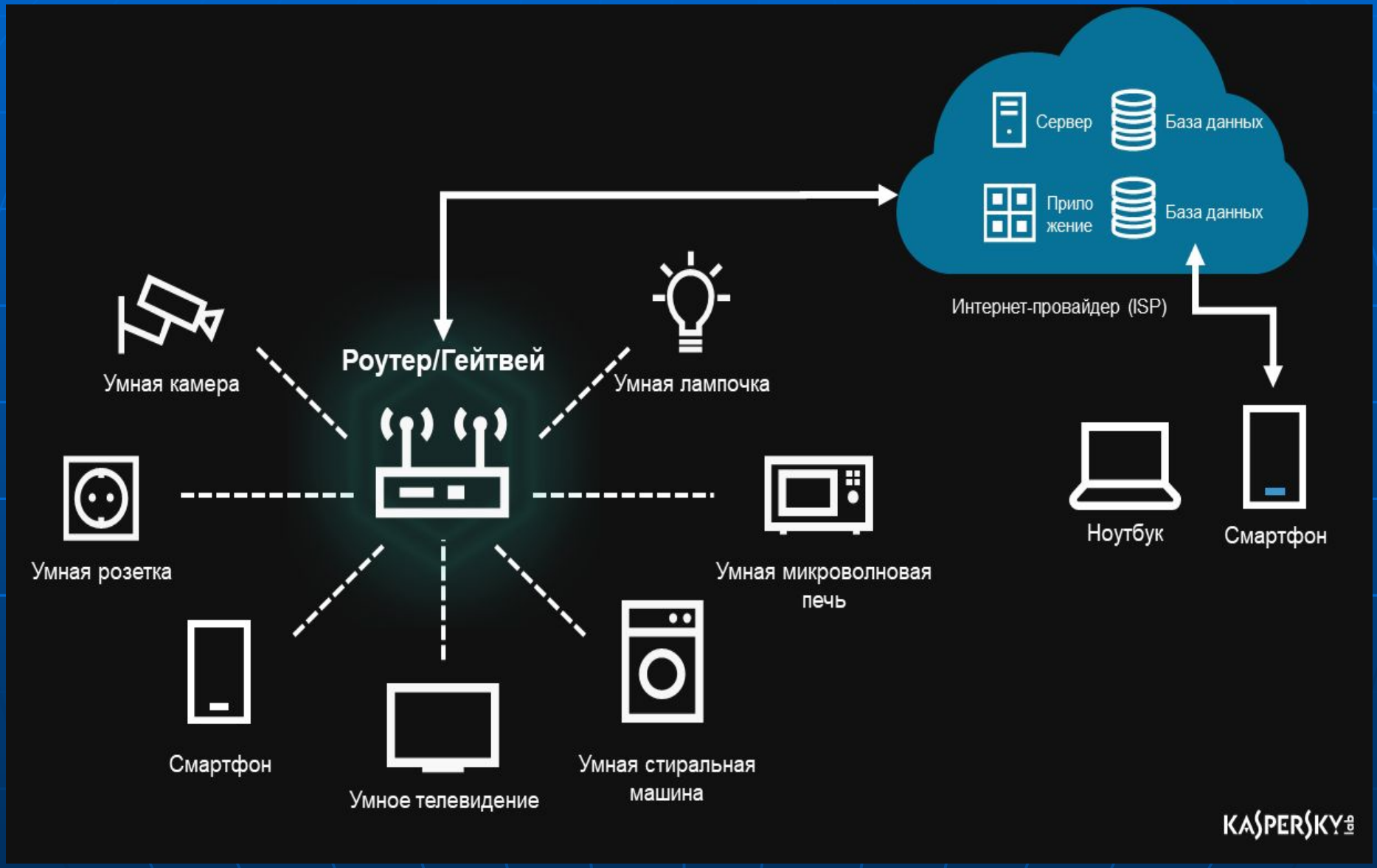
Как защититься от атак:

- *не переходите по ссылкам, полученным по почте от неизвестных отправителей или неизвестных веб-сайтов;*
- *избегайте незащищенных сетей Wi-Fi в общественных местах.*

3. Уязвимости интернета вещей

Интернет вещей (IoT) - сеть подключенных устройств, электрических бытовых приборов и других элементов с программным обеспечением, позволяющим им подключаться к Интернет


СЕТЕВЫЕ ТЕХНОЛОГИИ ДЛЯ IOT
логистика и транспорт
Управление автопарком
Отслеживание грузов
энергетические сети
Учет и мониторинг
Управление интеллектуальными сетями
сельское хозяйство
Мониторинг параметров окружающей среды
Управление запасами
умные города
Парковки
Городской транспорт
Освещение и др.
окружающая среда
Мониторинг состояния воздуха, водоемов и др.
умные дома
Пожарная и охранная сигнализация
Бытовая автоматизация
промышленность
Мониторинг и управление техническими процессами
пользовательская электроника
Носимые датчики
Мониторинг здоровья
Системы контроля местоположения


Сервер
База данных
Прило жение
База данных
Интернет-провайдер (ISP)
Роутер/Гейтвей
Умная камера
Умная лампочка
Умная розетка
Умная микроволновая печь
Ноутбук
Смартфон
Смартфон
Умное телевидение
Умная стиральная машина
KASPERSKY lab

Основные причины уязвимости IoT:

1. Слабые, легко угадываемые или запрограммированные пароли.

2. Небезопасные сетевые услуги.

3. Небезопасные интерфейсы экосистем.

4. Отсутствие надежного механизма обновления.

5. Использование небезопасных или устаревших компонентов.

6. Недостаточная защита конфиденциальности.

7. Небезопасная передача и хранение данных.

8. Отсутствие управления устройством.

9. Небезопасные настройки по умолчанию.

10. Отсутствие физической защиты устройств.

4. Центры мониторинга и управления безопасностью.

Центр мониторинга и оперативного управления безопасностью позволяет обеспечить:

- *мониторинг инцидентов информационной безопасности;*
- *реагирование на инциденты ИБ;*
- *контроль защищенности информационных систем;*
- *управление ИБ-системами организации.*

Используемые технологии разделяются на группы:

- *аудит событий;*
- *сбор, фильтрация и хранение событий;*
- *корреляция событий и выявление инцидентов;*
- *расследование инцидентов и эскалация проблем;*
- *отчетность на всех уровнях управления инцидентами.*

Выгоды:

- ***Создание центров мониторинга и управления безопасностью позволяет снизить ущерб от инцидентов ИБ за счет своевременного и эффективного реагирования и сбора доказательной базы.***

- ***Постоянный анализ событий и инцидентов безопасности, выяснение причин их возникновения позволяют оценить эффективность мер защиты, выявить их недостатки и выработать предложения по их замене или корректировке.***

Выгоды:

- ***С помощью Центра управления инцидентами безопасности реализуются нормативные и международные требования по мониторингу событий.***

- ***Централизация информации о состоянии ИБ в единой системе позволяет сократить расходы на аудит и контроль событий ИБ.***

5. Понятие Критической информационной инфраструктуры

Критическая информационная инфраструктура (КИИ) *- совокупность информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, которые на праве собственности, аренды или на ином законном основании принадлежат государственным органам и учреждениям, российским юридическим лицам и (или) индивидуальным предпринимателям, работающим в сфере здравоохранения, науки, транспорта, связи, энергетики, топливно-энергетического комплекса, в банковской сфере и иных сферах финансового рынка, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, а также российским юридическим лицам и (или) индивидуальным предпринимателям, которые обеспечивают взаимодействие указанных систем или сетей вкупе с сетями электросвязи, используемыми для организации взаимодействия таких объектов.*

187-ФЗ по тематике КИИ:
– вводит основные понятия;
– создает основу правового регулирования;
– определяет принципы обеспечения безопасности КИИ;
– вводит понятие Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА);
– вводит основу для создания Национального координационного центра по компьютерным инцидентам (НКЦКИ);

187-ФЗ по тематике КИИ:

– описывает полномочия Президента и органов госвласти в области обеспечения безопасности КИИ;

– содержит базу для определения категорий объектов КИИ;

– создает законодательную основу ведения реестра значимых объектов КИИ;

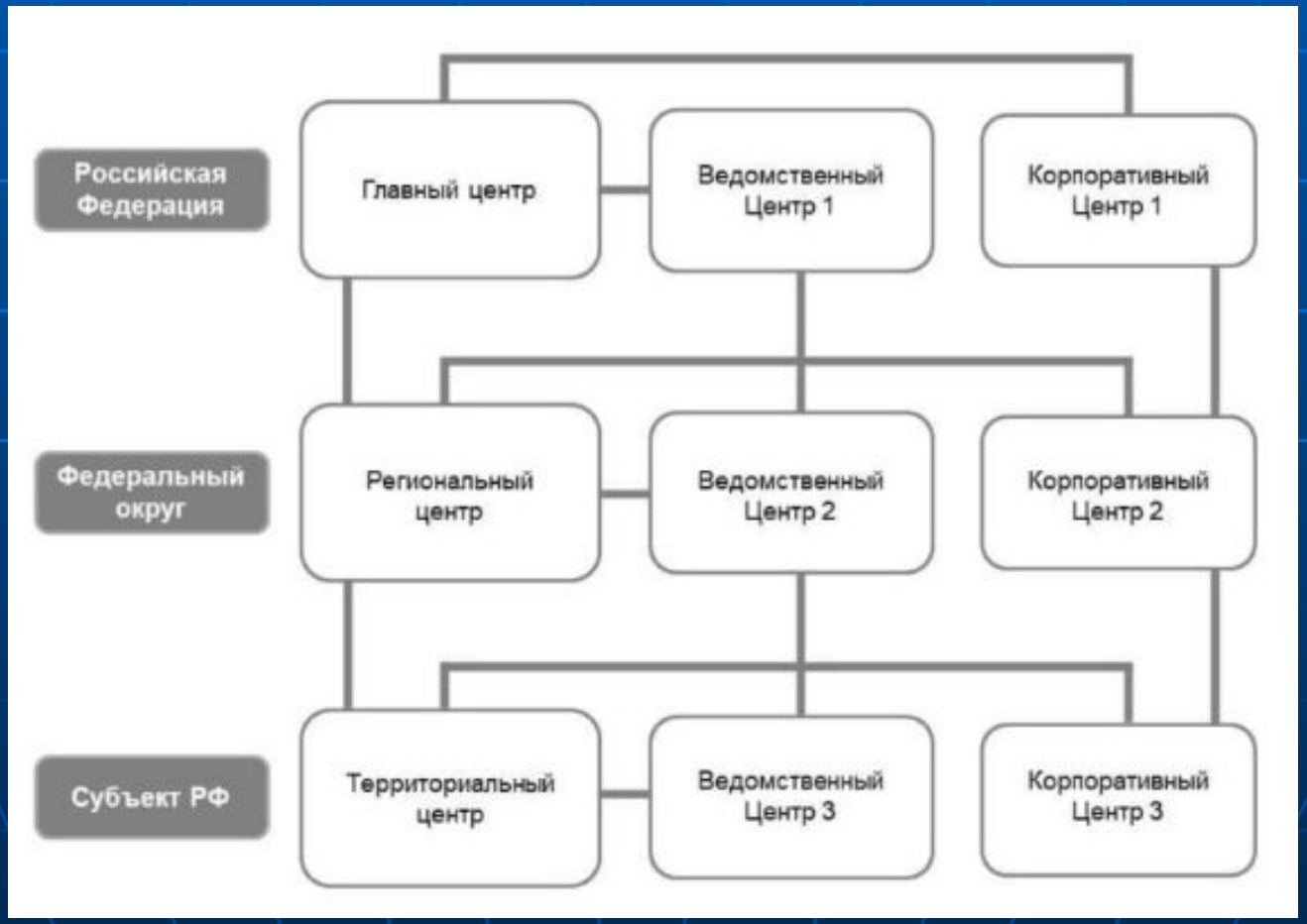
– определяет права и обязанности субъектов КИИ;

– определяет задачи и требования системы обеспечения безопасности значимого объекта КИИ;

– закладывает основу оценки безопасности КИИ;

– распределяет права и обязанности по государственному контролю.

ГосСОПКА — это единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.



Национальный координационный центр по компьютерным инцидентам (НКЦКИ) – структура, отвечающая за обеспечение координации деятельности субъектов КИИ, являющаюся составной частью ГосСОПКА

(Создан приказом ФСБ России №366 от 24 июля 2018 года «О Национальном координационном центре по компьютерным инцидентам»)

В функции НКЦКИ входит:
– Координация мероприятий и участие в мероприятиях по реагированию на компьютерные инциденты;
– Организует и осуществляет обмен информацией о компьютерных инцидентах;
– Осуществляет методическое обеспечение;
– Участвует в обнаружении, предупреждении и ликвидации последствий компьютерных атак;
– Обеспечивает информирование о компьютерных атаках;
– Собирает и анализирует информацию о компьютерных инцидентах и атаках.