

Лекция:

Государственная система обеспечения информационной безопасности РФ

Доцент кафедры прикладной информатики и информационной безопасности
к.т.н., доцент Карпов Д.С.

Учебные вопросы

1. Государственная система обеспечения информационной безопасности РФ.
2. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ
3. Центры реагирования на компьютерные инциденты в РФ
4. Федеральные государственные органы РФ, осуществляющие полномочия по предотвращению противоправных действий и борьбе с преступлениями в сфере компьютерной информации

Перечень основных нормативных правовых актов в области обеспечения создания и функционирования СОИБ РФ

1. Конституция Российской Федерации от 25.12.1993 года.
2. Стратегия национальной безопасности Российской Федерации (утв. Указом Президента РФ от 31.12.2015 N 683)
3. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры российской федерации (Утв. Президентом РФ 3 февраля 2012 г. N 803).
4. Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. (Утверждена Президентом РФ от 12.12.2014 № К 1274).
5. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ
6. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности».
7. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
8. Федеральный закон от 2 мая 2006 N 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»
9. Федеральный закон Российской Федерации от 28 декабря 2010 г. № 403-ФЗ «О Следственном комитете Российской Федерации».
10. Федеральный закон от 3 апреля 1995 г. № 40-ФЗ «О федеральной службе безопасности».
11. Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции».
12. Уголовный кодекс Российской Федерации (№ 63-ФЗ от 13 июня 1996 года).
13. Уголовно-процессуальный кодекс Российской Федерации (№ 174-ФЗ от 18 декабря 2001 года).

Перечень основных нормативных правовых актов в области обеспечения создания и функционирования СОИБ РФ

14. Указ Президента Российской Федерации от 15 января 2013 г. N 31с "О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации".

15. Указ Президента РФ от 22.05.2015 N 260 "О некоторых вопросах информационной безопасности Российской Федерации" (вместе с "Порядком подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети "Интернет" и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети "Интернет").

16. Приказ ФСТЭК от 14 марта 2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды

17. Информационное сообщение по вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры в связи с изданием приказа ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» от 25 июля 2014 г. № 240/22/2748

18. Приказ МВД России от 29.08.2014 N 736 «Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах МВД РФ заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях»

19. Приказ Председателя Следственного комитета РФ от 03.05.2011 года № 72 «Об утверждении Инструкции о порядке приема, регистрации и проверки сообщений о преступлении в следственных органах (следственных подразделениях) системы Следственного комитета РФ».

Вопрос 1

**Государственная система обеспечения
информационной безопасности РФ**

IV. Стратегические цели и основные направления обеспечения информационной безопасности

22. Стратегическими целями обеспечения информационной безопасности в области государственной и общественной безопасности являются защита суверенитета, поддержание политической и социальной стабильности, территориальной целостности Российской Федерации, обеспечение основных прав и свобод человека и гражданина, а также защита критической информационной инфраструктуры.

23. Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются:

...

в) повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической информационной инфраструктуры;

г) повышение безопасности функционирования объектов информационной инфраструктуры, в том числе в целях обеспечения устойчивого взаимодействия государственных органов, недопущения иностранного контроля за функционированием таких объектов, обеспечение целостности, устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации, а также обеспечение безопасности информации, передаваемой по ней и обрабатываемой в информационных системах на территории Российской Федерации;

д) повышение безопасности функционирования образцов вооружения, военной и специальной техники и автоматизированных систем управления;

...

Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 года N 646)

6. **Стратегической целью обеспечения информационной безопасности в области науки, технологий и образования является поддержка инновационного и ускоренного развития системы обеспечения информационной безопасности**, отрасли информационных технологий и электронной промышленности.

Система обеспечения информационной безопасности - совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности;

V. Организационные основы обеспечения информационной безопасности

30. **Система обеспечения информационной безопасности** является частью системы обеспечения национальной безопасности Российской Федерации.

Обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами.

31. **Система обеспечения информационной безопасности** строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере с учетом предметов ведения федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, а также органов местного самоуправления, определяемых законодательством Российской Федерации в области обеспечения безопасности.

Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 года N 646)

32. Состав системы обеспечения информационной безопасности определяется Президентом Российской Федерации.

33. Организационную основу системы обеспечения информационной безопасности составляют: Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, Центральный банк Российской Федерации, Военно-промышленная комиссия Российской Федерации, межведомственные органы, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, принимающие в соответствии с законодательством Российской Федерации участие в решении задач по обеспечению информационной безопасности.

Участниками системы обеспечения информационной безопасности являются: собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты, средства массовой информации и массовых коммуникаций, организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка, операторы связи, операторы информационных систем, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, организации, осуществляющие образовательную деятельность в данной области, общественные объединения, иные организации и граждане, которые в соответствии с законодательством Российской Федерации участвуют в решении задач по обеспечению информационной безопасности.

Элементы системы обеспечения информационной безопасности

Федеральные органы исполнительной власти РФ — федеральные министерства (21), федеральные службы (28), федеральные агентства (22).

Федеральные агентства, федеральные министерства и федеральные службы отличаются:

1. по объему полномочий

Министерства:

- выработка гос. политики в определенной отрасли, т.е. ставит цели и способы их достижения;
- установление правил, нормативов (СНиПы, ГОСТы, тарифы, СанПиНы и т.п.);
- контроль над деятельностью подведомственных учреждений, служб и агентств.

Министерства действуют в определенной сфере: здравоохранения, обороны, культуры, спорта и туризма, образования и т.п.

Агентства:

- осуществление в установленной сфере деятельности функций по оказанию государственных услуг, по управлению государственным имуществом и правоприменительных функций, за исключением функций по контролю и надзору.

Службы:

- осуществление функций по контролю и надзору в установленной сфере деятельности.

2. по подчиненности

Министерства подчиняются правительству.

Агентства могут подчиняться:

- Президенту РФ;
- Правительству РФ;
- федеральным министерствам.

Федеральные службы подчиняются соответствующим федеральным министерствам, но некоторые напрямую подчиняются Президенту или Правительству России.

Военно-промышленная комиссия Российской Федерации (ВПК России) — постоянно действующий орган, образованный в целях организации государственной политики в сфере оборонно-промышленного комплекса, военно-технического обеспечения обороны страны, безопасности государства и правоохранительной деятельности.

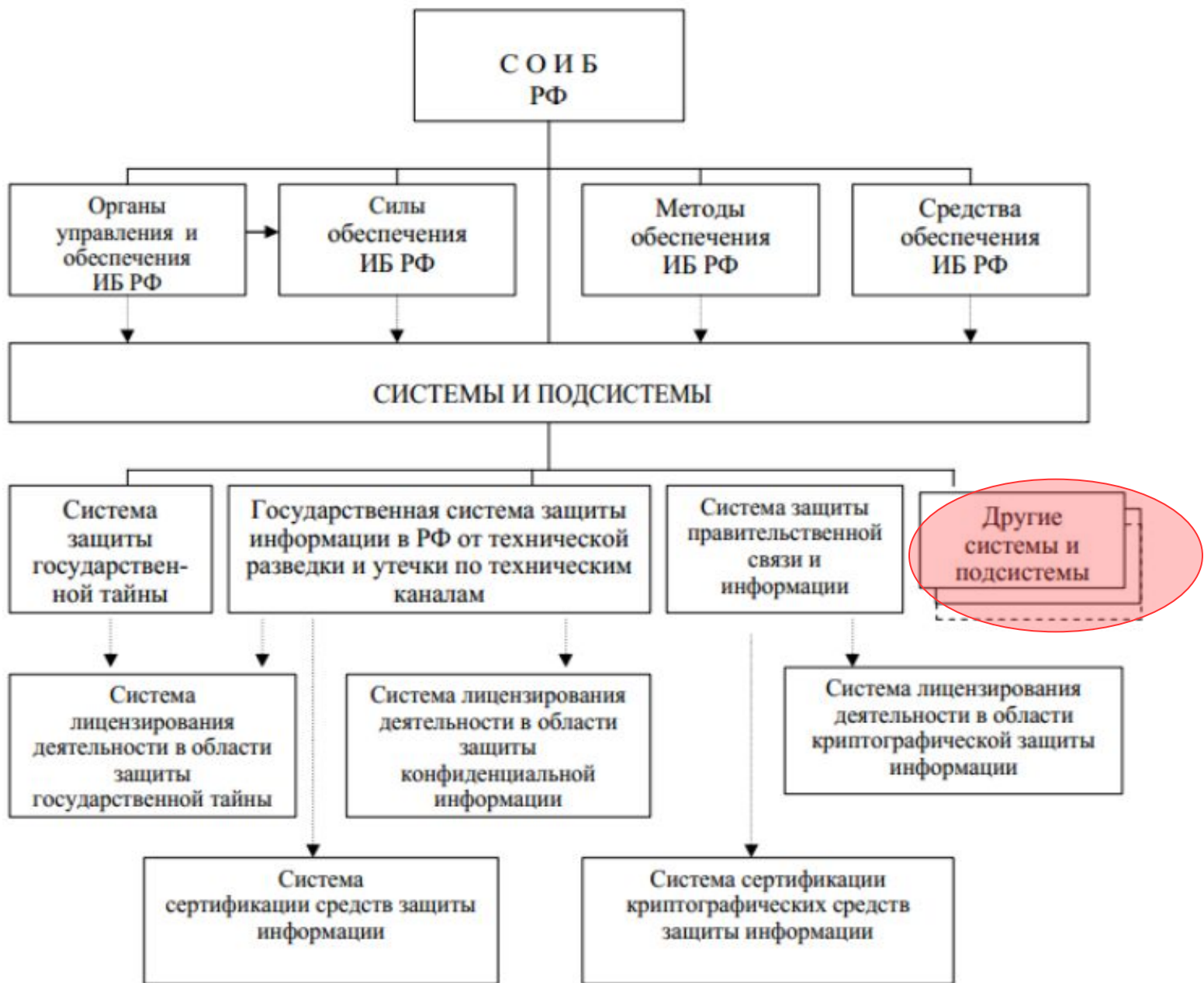
Образована в 1999 году как Комиссия по военно-промышленным вопросам Правительства РФ, в 2006 году переименована в ВПК, в 2014 году переподчинена Президенту. В 2007 году комиссия получила право формировать гос. заказ в сфере обороны.

Межведомственная комиссия по защите государственной тайны - коллегиальный орган, основной функцией которого является координация деятельности федеральных органов исполнительной власти и органов государственной власти субъектов РФ по защите государственной тайны в интересах разработки и выполнения государственных программ, нормативных и методических документов, обеспечивающих реализацию федерального законодательства о государственной тайне.

Межведомственная комиссия осуществляет также функцию по рассекречиванию документов, созданных КПСС.

Межведомственная комиссия Совета Безопасности Российской Федерации по информационной безопасности образована в целях реализации возложенных на СБ РФ задач в области обеспечения информационной безопасности Российской Федерации в соответствии с Федеральным законом от 28 декабря 2010 г. N 390-ФЗ "О безопасности" и Положением о Совете Безопасности Российской Федерации.

Состав системы обеспечения информационной безопасности РФ



Основные элементы системы обеспечения информационной безопасности РФ

1. Комитет Государственной Думы по безопасности и противодействию коррупции.
2. Комитет Совета Федерации по обороне и безопасности
3. Совет Безопасности РФ.
4. Министерство внутренних дел Российской Федерации.
5. Следственный комитет Российской Федерации.
6. Федеральная служба безопасности России.
7. Федеральная служба по техническому и экспортному контролю
8. Министерство связи и массовых коммуникаций РФ.
9. Координационный центр национального домена сети Интернет
10. Центры реагирования на компьютерные инциденты в информационных системах.
11. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (ГосСОПКА)

Комитет Совета Федерации по обороне и безопасности

К важнейшим вопросам ведения Комитета относятся: правовое регулирование внутренней и внешней безопасности, военного строительства, охраны и защиты государственной границы, финансирования военной организации государства, поддержание правопорядка и законности.

Особое внимание Комитет уделяет правовому обеспечению развития оборонно-промышленного комплекса, реформирования вооруженных сил, включая улучшение социальной защищенности военнослужащих и сотрудников правоохранительных органов, борьбы с терроризмом и организованной преступностью.

Комитет Государственной Думы по безопасности и противодействию коррупции

Вопросы ведения Комитета

6.1. Предварительное рассмотрение и подготовка к рассмотрению Государственной Думой законопроектов и проектов постановлений палаты по следующим вопросам:

6.1.1. О статусе и правовом регулировании деятельности:

...

Об информационной безопасности личности, общества и государства (защита информации, составляющей государственную, служебную и коммерческую тайну, защита персональных данных, информационно-психологическая безопасность человека).

6.1.11. Об основах предупреждения преступности, привлечения населения к охране правопорядка, профилактики девиантного поведения, представляющего угрозу безопасности граждан и общества (наркомания, преступность несовершеннолетних, алкоголизм).

...

6.3.3. Участие в разработке правовых основ геополитических интересов Российской Федерации, направленных на укрепление национальной безопасности Российской Федерации (правовые меры противодействия геополитическим устремлениям иностранных государств, которые могут нанести ущерб внутренней и внешней безопасности, национальному достоянию и другим государственным интересам Российской Федерации, включая сферу международных отношений).

...

Таким образом, в РФ сформирована и действует система обеспечения информационной безопасности (СОИБ РФ).

СОИБ является совокупностью сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности.

В состав СОИБ наряду с другими важнейшими подсистемами входит система противодействия преступлениям в сфере компьютерной информации в РФ в состав которой, в свою очередь, входит ГосСОПКА.

Одной из главных стратегических целей обеспечения информационной безопасности РФ является поддержка инновационного и ускоренного развития системы обеспечения информационной безопасности.

Вопрос 2

**Государственная система обнаружения,
предупреждения и ликвидации последствий
компьютерных атак на информационные
ресурсы РФ**

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

В январе 2013 года был подписан указ о создании в России государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА).

В 2015 году появились первые ведомственные центры ГосСОПКА, в 2016-м — корпоративные.

Планируется, что к системе ГосСОПКА должны подключиться все федеральные органы власти, а также объекты критической информационной инфраструктуры РФ.

Необходимость подключения к ГосСОПКА в явном виде указана в Федеральном законе N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации", который был принят 26.07.2017.

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ

Основные НПА

1. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (Утв. Президентом РФ Д. Медведевым 3 февраля 2012 г. N 803).

2. Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, утвержденная Президентом РФ 12.12.2014 № К 1274.

http://www.fsb.ru/files/PDF/Vipiska_iz_koncepcii.pdf

3. Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ

4. Указ Президента Российской Федерации от 15 января 2013 г. N 31с "О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации".

5. Указ Президента РФ от 22.05.2015 N 260 "О некоторых вопросах информационной безопасности Российской Федерации" (вместе с "Порядком подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети "Интернет" и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети "Интернет").

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

7. Указ Президента РФ от 16.08.2004 N 1085 (ред. от 08.05.2018) "Вопросы Федеральной службы по техническому и экспортному контролю" ...

Основные НПА

8. Постановление Правительства РФ №127 от 08.02.2018 «Об утверждении Правил категорирования объектов КИИ РФ, а также перечня показателей критериев значимости объектов КИИ РФ и их значений»
9. Постановление Правительства РФ №162 от 17.02.2018 «Об утверждении Правил осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ»
10. Приказ Федеральной службы по техническому и экспортному контролю от 06.12.2017 №227 «Об утверждении Порядка ведения реестра значимых объектов КИИ РФ»
11. Приказ Федеральной службы по техническому и экспортному контролю от 11.12.2017 №229 «Об утверждении формы акта проверки, составляемого по итогам проведения госконтроля в области обеспечения безопасности значимых объектов КИИ РФ»
12. Приказ Федеральной службы по техническому и экспортному контролю от 21.12.2017 №235 «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования»
13. Приказ Федеральной службы по техническому и экспортному контролю от 22.12.2017 № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»
14. Приказ Федеральной службы по техническому и экспортному контролю от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»
15. Методические рекомендации по созданию ведомственных и корпоративных центров ГосСОПКА от Центра защиты информации и специальной связи ФСБ России №149/2/7-200 от 24.12.2016
16. Методика отнесения объектов государственной и негосударственной собственности к критически важным объектам для национальной безопасности Российской Федерации (утв. Зам. Министра РФ по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий 17 октября 2012 года N 2-4-87-23-14)

Стратегия национальной безопасности Российской Федерации (утв. Указом Президента РФ от 31.12.2015 N 683)

IV. Обеспечение национальной безопасности

...

Государственная и общественная безопасность

...

43. Основными угрозами государственной и общественной безопасности являются:

разведывательная и иная деятельность специальных служб и организаций иностранных государств, отдельных лиц, наносящая ущерб национальным интересам;

деятельность террористических и экстремистских организаций, направленная на насильственное изменение конституционного строя Российской Федерации, дестабилизацию работы органов государственной власти, уничтожение или нарушение функционирования военных и промышленных объектов, объектов жизнеобеспечения населения, транспортной инфраструктуры, устрашение населения, в том числе путем завладения оружием массового уничтожения, радиоактивными, отравляющими, токсичными, химически и биологически опасными веществами, совершения актов ядерного терроризма, нарушения безопасности и устойчивости функционирования критической информационной инфраструктуры Российской Федерации;

47. В целях обеспечения государственной и общественной безопасности:

...

укрепляется режим безопасного функционирования, повышается уровень антитеррористической защищенности организаций оборонно-промышленного, ядерного, химического, топливно-энергетического комплексов страны, объектов жизнеобеспечения населения, транспортной инфраструктуры, других критически важных и потенциально опасных объектов;

Основные направления государственной политики в области обеспечения безопасности АСУ производственными и технологическими процессами критически важных объектов инфраструктуры РФ (утв. Президентом Российской Федерации Д. Медведевым 03.02.2012 г. N 803)

I. Общие положения

Основные направления разработаны в целях реализации основных положений Стратегии национальной безопасности Российской Федерации до 2020 года*, в соответствии с которой одним из путей предотвращения угроз информационной безопасности Российской Федерации является совершенствование безопасности функционирования информационных и телекоммуникационных систем критически важных объектов инфраструктуры и объектов повышенной опасности в Российской Федерации.

2. Целью государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации является снижение до минимально возможного уровня рисков неконтролируемого вмешательства в процессы функционирования данных систем, а также минимизация негативных последствий подобного вмешательства.

Основные направления государственной политики в области обеспечения безопасности АСУ производственными и технологическими процессами критически важных объектов инфраструктуры РФ (утв. Президентом РФ 03.02.2012 г. N 803)

3. Основные понятия, используемые в настоящих Основных направлениях:

а) **критически важный объект инфраструктуры РФ (далее - критически важный объект)** - объект, нарушение (или прекращение) функционирования которого приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению (или разрушению) экономики страны, субъекта РФ либо административно-территориальной единицы или существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный срок;

б) **автоматизированная система управления производственными и технологическими процессами критически важного объекта инфраструктуры РФ (далее - автоматизированная система управления КВО)** - комплекс аппаратных и программных средств, информационных систем и информационно-телекоммуникационных сетей, предназначенных для решения задач оперативного управления и контроля за различными процессами и техническими объектами в рамках организации производства или технологического процесса критически важного объекта, нарушение (или прекращение) функционирования которых может нанести вред внешнеполитическим интересам РФ, стать причиной аварий и катастроф, массовых беспорядков, длительных остановок транспорта, производственных или технологических процессов, дезорганизации работы учреждений, предприятий или организаций, нанесения материального ущерба в крупном размере, смерти или нанесения тяжкого вреда здоровью хотя бы одного человека и (или) иных тяжелых последствий (далее - тяжкие последствия);

в) **критическая информационная инфраструктура РФ (далее - критическая информационная инфраструктура)** - совокупность автоматизированных систем управления КВО и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей, предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка, нарушение (или прекращение) функционирования которых может стать причиной наступления тяжких последствий;

г) **компьютерная атака** - целенаправленное воздействие на информационные системы и информационно-телекоммуникационные сети программно-техническими средствами, осуществляемое в целях нарушения безопасности информации в этих системах и сетях;

Основные направления государственной политики в области обеспечения безопасности АСУ производственными и технологическими процессами критически важных объектов инфраструктуры РФ (утв. Президентом РФ 03.02.2012 г. N 803)

2
3

3. Основные понятия, используемые в настоящих Основных направлениях: (продолжение)

...

д) **безопасность автоматизированной системы управления КВО** - состояние автоматизированной системы управления КВО, при котором обеспечивается соблюдение проектных пределов значений параметров выполнения ею целевых функций (далее - штатный режим функционирования) при проведении в отношении ее компьютерных атак;

е) **безопасность критической информационной инфраструктуры** - состояние элементов критической информационной инфраструктуры и критической информационной инфраструктуры в целом, при котором проведение в отношении ее компьютерных атак не влечет за собой тяжких последствий;

ж) **компьютерный инцидент** - факт нарушения штатного режима функционирования элемента критической информационной инфраструктуры или критической информационной инфраструктуры в целом;

з) **единая государственная система обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру и оценки уровня реальной защищенности ее элементов** - централизованная, иерархическая, территориально распределенная структура, включающая силы и средства обнаружения и предупреждения компьютерных атак, а также органы управления различных уровней, в полномочия которых входят вопросы обеспечения безопасности автоматизированных систем управления КВО и иных элементов критической информационной инфраструктуры;

и) **силы обнаружения и предупреждения компьютерных атак** - уполномоченные подразделения федерального органа исполнительной власти в области обеспечения безопасности, федеральных органов исполнительной власти, осуществляющих деятельность в области обеспечения безопасности, государственного надзора и контроля, управления деятельностью критически важных объектов и иных элементов критической информационной инфраструктуры, а также физические лица и специально выделенные сотрудники организаций, осуществляющих эксплуатацию автоматизированных систем управления КВО и иных элементов критической информационной инфраструктуры на правах собственности либо на иных законных основаниях, принимающие участие в обнаружении и предупреждении компьютерных атак на критическую информационную инфраструктуру, мониторинге уровня ее реальной защищенности и ликвидации последствий компьютерных инцидентов на основании законодательства Российской Федерации;

Основные направления государственной политики в области обеспечения безопасности АСУ производственными и технологическими процессами критически важных объектов инфраструктуры РФ (утв. Президентом РФ 03.02.2012 г. N 803)

3. Основные понятия, используемые в настоящих Основных направлениях: (продолжение)

...

к) **средства обнаружения и предупреждения 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 и предупреждения компьютерных атак на критическую информационную инфраструктуру, мониторинга уровня ее реальной защищенности и ликвидации последствий компьютерных инцидентов;

л) **силы ликвидации последствий компьютерных инцидентов в критической информационной инфраструктуре** - уполномоченные подразделения федерального органа исполнительной власти в области обеспечения безопасности, физические лица и специально выделенные сотрудники организаций, осуществляющих эксплуатацию автоматизированных систем управления КВО и иных элементов критической информационной инфраструктуры на правах собственности либо на иных законных основаниях, а также сотрудники предприятий - разработчиков аппаратных средств и программного обеспечения, используемых в автоматизированных системах управления КВО, принимающие на основании законодательства Российской Федерации участие в восстановлении штатного режима функционирования элементов критической информационной инфраструктуры после компьютерных инцидентов;

м) **средства ликвидации последствий компьютерных инцидентов в критической информационной инфраструктуре** - технологии, а также технические, программные, правовые, организационные средства, включая сети и средства связи, средства сбора и анализа информации, предназначенные для восстановления штатного режима функционирования элементов критической информационной инфраструктуры после компьютерных инцидентов.

Основные направления государственной политики в области обеспечения безопасности АСУ производственными и технологическими процессами критически важных объектов инфраструктуры РФ (утв. Президентом РФ 03.02.2012 г. N 803)

II. Факторы, влияющие на формирование государственной политики в области обеспечения безопасности автоматизированных систем управления КВО, и ее основные принципы

4. Обеспечение безопасности автоматизированных систем управления КВО является невозможным без обеспечения безопасности автоматизированных систем управления КВО и критической информационной инфраструктуры в целом. Данное положение обусловлено повсеместным внедрением широкого спектра информационных технологий в системы управления производственными и технологическими процессами КВО, глобализацией современных информационно-телекоммуникационных сетей, превращением их в единую мировую информационно-телекоммуникационную сеть с размытыми границами национальных сегментов, существенным увеличением доли распределенных автоматизированных систем управления КВО и все большим использованием информационно-телекоммуникационных сетей и сетей связи общего использования для их информационного обмена.

5. Факторы, влияющие на формирование государственной политики в области обеспечения безопасности автоматизированных систем управления КВО:

- а) интеграция в единые комплексы автоматизированных систем управления КВО и других информационных систем, используемых в управлении производственными и транспортными структурами, административными и финансовыми ресурсами;
- б) постоянное усложнение используемых в автоматизированных системах управления КВО программного обеспечения и оборудования;
- в) практика осуществления иностранными фирмами технического обслуживания и удаленной настройки автоматизированных систем управления КВО в целом или их составных частей, а также телекоммуникационного оборудования, входящего в состав критической информационной инфраструктуры;
- г) стремление организаций - разработчиков программного обеспечения автоматизированных систем управления КВО к снижению издержек и, как следствие, использованию типовых решений и заимствованного программного обеспечения;

Основные направления государственной политики в области обеспечения безопасности АСУ производственными и технологическими процессами критически важных объектов инфраструктуры РФ (утв. Президентом РФ 03.02.2012 г. N 803)

5. Факторы, влияющие на формирование государственной политики в области обеспечения безопасности автоматизированных систем управления КВО: (продолжение)

д) интенсивное совершенствование средств и методов использования информационных и коммуникационных технологий для нанесения ущерба Российской Федерации, а также участвовавшие попытки их применения в противоправных целях и конкурентной борьбе;

е) усиление угрозы терроризма, рост числа противоправных деяний с использованием информационных и коммуникационных технологий;

ж) сложившаяся среди операторов и владельцев информационных систем, в состав которых входят автоматизированные системы управления КВО, тенденция сокрытия попыток или фактов нарушения их штатного функционирования;

з) недостаточный уровень образования и профессиональной подготовки персонала, обслуживающего автоматизированные системы управления КВО, снижение технологической культуры производства;

и) отсутствие достаточного нормативно-правового регулирования процессов обеспечения безопасности автоматизированных систем управления КВО, в том числе в части определения уровня их реальной защищенности;

к) вынужденное привлечение при создании автоматизированных систем управления КВО иностранных фирм - производителей и поставщиков программно-аппаратных средств обработки, хранения и передачи информации и применение зарубежных программно-аппаратных решений, создающих предпосылки для возникновения технологической и иной зависимости от иностранных государств.

Основные направления государственной политики в области обеспечения безопасности АСУ производственными и технологическими процессами критически важных объектов инфраструктуры РФ (утв. Президентом РФ 03.02.2012 г. N 803)

6. Основные принципы государственной политики в области обеспечения безопасности автоматизированных систем управления КВО:

- а) соблюдение законодательства РФ, а также требований международных договоров РФ всеми участниками процесса создания и эксплуатации автоматизированных систем управления КВО;
- б) сочетание интересов и взаимной ответственности государства, граждан, а также организаций, участвующих в разработке, создании и эксплуатации автоматизированных систем управления КВО;
- в) персонификация ответственности должностных лиц, операторов, персонала и иных лиц, принимающих участие в разработке, создании, вводе в действие, эксплуатации и модернизации АСУ КВО;
- г) обеспечение комплексной защиты критической информационной инфраструктуры в целом, включая создание единой государственной системы обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру и оценки уровня реальной защищенности ее элементов;
- д) обеспечение разрешительного характера деятельности в области обеспечения безопасности автоматизированных систем управления КВО с использованием механизмов лицензирования и сертификации;
- е) разделение функций между федеральным органом исполнительной власти в области обеспечения безопасности и иными федеральными органами исполнительной власти, осуществляющими деятельность в области безопасности, органами государственного надзора и контроля, управления деятельностью критически важных объектов и иных элементов критической информационной инфраструктуры, усиление координации их деятельности;
- ж) регламентация прав и обязанностей собственников автоматизированных систем управления КВО и иных объектов критической информационной инфраструктуры, а также эксплуатирующих их организаций;
- з) недопущение технологической или иной зависимости от иностранных государств при осуществлении деятельности в области обеспечения безопасности АСУ КВО.

7. Решение основных задач государственной политики в области обеспечения безопасности АСУ КВО должно осуществляться по следующим направлениям:

- а) совершенствование нормативно-правовой базы;
- б) государственное регулирование;
- в) промышленная и научно-техническая политика;
- г) фундаментальная и прикладная наука, технологии и средства обеспечения безопасности АСУ КВО и критической информационной инфраструктуры;
- д) повышение квалификации кадров в области обеспечения безопасности АСУ КВО.

Основные направления государственной политики в области обеспечения безопасности АСУ производственными и технологическими процессами критически важных объектов инфраструктуры РФ (утв. Президентом РФ 03.02.2012 г. N 803)

8. Основные задачи, касающиеся совершенствования нормативно-правовой базы в области обеспечения безопасности автоматизированных систем управления КВО:

а) определение и разграничение полномочий федерального органа исполнительной власти в области обеспечения безопасности, иных федеральных органов исполнительной власти, осуществляющих деятельность в области обеспечения безопасности, органов государственного надзора и контроля, управления деятельностью критически важных объектов и иных элементов критической информационной инфраструктуры;

б) **законодательное определение и закрепление прав и обязанностей собственников** автоматизированных систем управления КВО и иных объектов критической информационной инфраструктуры **и эксплуатирующих их организаций** в области обеспечения безопасности автоматизированных систем управления КВО;

в) **определение порядка:**

разработки, ввода в действие, эксплуатации и модернизации автоматизированных систем управления КВО и иных элементов критической информационной инфраструктуры;

получения федеральным органом исполнительной власти в области обеспечения безопасности информации об автоматизированных системах управления КВО и иных элементах критической информационной инфраструктуры;

использования сил и средств обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру;

использования сил и средств ликвидации последствий компьютерных инцидентов в критической информационной инфраструктуре;

действий должностных лиц, персонала и владельцев автоматизированных систем управления КВО и иных элементов критической информационной инфраструктуры при обнаружении попыток или фактов нарушения штатного функционирования этих объектов в случае компьютерных инцидентов;

г) **создание правовых оснований и определение порядка применения мер принудительного изменения информационного обмена с объектами информатизации, являющимися источниками компьютерных атак, вплоть до его полного прекращения;**

д) **нормативно-правовое обеспечение функционирования единой государственной системы обнаружения компьютерных атак на критическую информационную инфраструктуру и мониторинга уровня ее реальной защищенности;**

е) **введение ответственности** за нарушение порядка разработки, ввода в действие, эксплуатации и модернизации автоматизированных систем управления КВО и иных элементов критической информационной инфраструктуры;

ж) **усиление ответственности за создание и (или) применение средств компьютерных атак;**

з) оптимизация законодательства Российской Федерации в части лицензирования деятельности, связанной с разработкой, производством, эксплуатацией и техническим обслуживанием автоматизированных систем управления критически важными объектами.

Основные направления государственной политики в области обеспечения безопасности АСУ производственными и технологическими процессами критически важных объектов инфраструктуры РФ (утв. Президентом РФ 03.02.2012 г. N 803)

9. Основные задачи государственного регулирования в области обеспечения безопасности автоматизированных систем управления КВО:

- а) развитие механизмов государственного управления и контроля, а также усиление координации в области обеспечения безопасности критической информационной инфраструктуры;
- б) выделение (привлечение) необходимых объемов и источников финансовых ресурсов (бюджетных и внебюджетных) на реализацию программ и планов мероприятий в области обеспечения безопасности автоматизированных систем управления КВО и критической информационной инфраструктуры в целом;
- в) создание единой государственной системы обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру и оценки защищенности ее элементов;
- г) обеспечение устойчивого функционирования национального сегмента единой мировой информационно-телекоммуникационной сети в условиях массированного деструктивного информационного воздействия с территорий, находящихся вне юрисдикции Российской Федерации;
- д) создание условий, стимулирующих развитие на территории Российской Федерации производства телекоммуникационного оборудования, устойчивого к компьютерным атакам;
- е) создание и поддержание в постоянной готовности сил и средств ликвидации последствий компьютерных инцидентов в критической информационной инфраструктуре;
- ж) развитие международного сотрудничества, включая совершенствование международной кооперации в области обеспечения информационной безопасности;
- з) стимулирование, в том числе материальное, проведения частными организациями и лицами исследований в области обнаружения уязвимостей программного обеспечения и оборудования, применяемого в автоматизированных системах управления КВО и на иных объектах критической информационной инфраструктуры, с представлением результатов федеральному органу исполнительной власти в области обеспечения безопасности.

Основные направления государственной политики в области обеспечения безопасности АСУ производственными и технологическими процессами критически важных объектов инфраструктуры РФ (утв. Президентом РФ 03.02.2012 г. N 803)

10. Основные задачи по совершенствованию промышленной и научно-технической политики в области обеспечения безопасности автоматизированных систем управления КВО:

а) проведение комплекса мероприятий по развитию систем, средств и методов технической оценки уровня реальной защищенности автоматизированных систем управления КВО и критической информационной инфраструктуры в целом;

б) создание единых реестров программных и аппаратных средств, используемых в автоматизированных системах управления КВО, создание баз данных, касающихся надежности функционирования автоматизированных систем управления КВО, состояния их защищенности, состояния технического оборудования, оценки эффективности действующих и внедряемых на критически важных объектах мер безопасности;

в) проведение комплекса организационно-технических мероприятий по исключению прохождения информационного обмена автоматизированных систем управления КВО по территориям иностранных государств, а при технической невозможности такого исключения - создание и применение защитных мер, обеспечивающих отсутствие любых негативных воздействий на процессы, контролируемые автоматизированными системами управления КВО, в случае нарушения штатного функционирования этого канала связи;

г) разработка комплекса мер по созданию и внедрению телекоммуникационного оборудования, устойчивого к компьютерным атакам;

д) создание хранилища эталонного программного обеспечения, используемого в автоматизированных системах управления КВО и на других объектах критической информационной инфраструктуры;

е) развитие (с учетом мобилизационной готовности) научно-производственной базы, обеспечивающей выпуск систем (средств) обеспечения безопасности автоматизированных систем управления КВО и иных объектов критической информационной инфраструктуры;

ж) разработка и внедрение импортозамещающих технологий, материалов, комплектующих и других видов продукции, используемых в автоматизированных системах управления КВО.

Основные направления государственной политики в области обеспечения безопасности АСУ производственными и технологическими процессами критически важных объектов инфраструктуры РФ (утв. Президентом РФ 03.02.2012 г. N 803)

11. Основные задачи в области развития фундаментальной и прикладной науки, технологий и средств обеспечения безопасности автоматизированных систем управления КВО и критической информационной инфраструктуры:

а) разработка методов и средств своевременного выявления угроз и оценки их опасности для автоматизированных систем управления КВО и иных элементов критической информационной инфраструктуры;

б) разработка и внедрение специализированных информационно-аналитических систем, развитие исследований в области математического моделирования процессов обеспечения безопасности автоматизированных систем управления КВО и иных объектов критической информационной инфраструктуры, направленных на выработку вероятных сценариев развития ситуации и поддержку управленческих решений;

в) разработка и внедрение комплексных систем защиты и обеспечения безопасности автоматизированных систем управления КВО и иных объектов критической информационной инфраструктуры, отвечающих современному уровню развития информационных технологий и минимизирующих участие обслуживающего персонала в настройке и эксплуатации входящих в их состав программно-аппаратных средств;

г) разработка для автоматизированных систем управления КВО специализированных экономически целесообразных информационных технологий, исключаящих или в максимальной степени снижающих на технологическом уровне обмен информацией, подлежащей обязательной защите.

12. Основные задачи по совершенствованию образования, подготовки и повышения квалификации кадров в области обеспечения безопасности автоматизированных систем управления КВО, повышению общего уровня культуры информационной безопасности граждан:

а) совершенствование системы подготовки, переподготовки и аттестации кадров (в том числе руководящих) в области обеспечения безопасности автоматизированных систем управления КВО и критической информационной инфраструктуры на базе профильных образовательных учреждений;

б) повышение общего уровня культуры информационной безопасности граждан, включая повышение информированности населения о критической информационной инфраструктуре, угрозах информационной безопасности и способах защиты от этих угроз;

в) формирование в общественном сознании нетерпимости к лицам, совершающим противоправные деяния с использованием информационных технологий.

Основные направления государственной политики в области обеспечения безопасности АСУ производственными и технологическими процессами критически важных объектов инфраструктуры РФ (утв. Президентом РФ 03.02.2012 г. N 803)

IV. Основные механизмы и этапы реализации государственной политики в области обеспечения безопасности автоматизированных систем управления КВО

13. Реализация настоящих Основных направлений обеспечивается путем консолидации усилий органов государственной власти и институтов гражданского общества, направленных на защиту интересов РФ посредством комплексного использования правовых, организационных, технических, социально-экономических, специальных и иных мер поддержки.

14. **Координацию деятельности федеральных органов исполнительной власти по реализации настоящих Основных направлений осуществляет федеральный орган исполнительной власти в области обеспечения безопасности.**

15. **Настоящие Основные направления реализуются в рамках:**

- а) существующих и планируемых государственных программ;
- б) плана мероприятий по реализации наст. Основных направлений, утверждаемого Правительством РФ.

16. **Настоящие Основные направления реализуются поэтапно.**

17. **На первом этапе (2012 - 2013 годы) необходимо осуществить:**

- а) **подготовку плана мероприятий** по реализации настоящих Основных направлений;
- б) **нормативно-правовое определение и разграничение полномочий и ответственности** федерального органа исполнительной власти в области обеспечения безопасности, иных федеральных органов исполнительной власти, осуществляющих деятельность в области обеспечения безопасности, органов государственного надзора и контроля, управления деятельностью КВО и объектов критической информационной инфраструктуры;
- в) **определение порядка использования сил и средств обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру;**
- г) **разработку концепции использования сил и средств ликвидации последствий компьютерных инцидентов в критической информационной инфраструктуре;**
- д) **определение необходимых объемов и источников финансовых ресурсов** (бюджетных и внебюджетных) на реализацию программ и планов мероприятий в области обеспечения безопасности автоматизированных систем управления КВО и критической информационной инфраструктуры в целом на период второго этапа реализации настоящих Основных направлений;
- е) **подготовку предложений по внесению изменений в утвержденные государственные программы и корректировке планируемых государственных программ.**

Основные направления государственной политики в области обеспечения безопасности АСУ производственными и технологическими процессами критически важных объектов инфраструктуры РФ (утв. Президентом РФ 03.02.2012 г. N 803)

18. На втором этапе (2014 - 2016 годы) необходимо осуществить:

а) разработку нормативных правовых актов, определяющих:

- порядок получения федеральным органом исполнительной власти в области обеспечения безопасности информации об АСУ КВО и иных объектах критической информационной инфраструктуры;
- права и обязанности собственников автоматизированных систем управления КВО и иных объектов критической информационной инфраструктуры, а также эксплуатирующих их организаций в области обеспечения их безопасности;
- порядок разработки, ввода в действие, эксплуатации и модернизации автоматизированных систем управления КВО;
- регламент функционирования единой государственной системы обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру и оценки защищенности ее элементов;
- порядок ликвидации последствий компьютерных инцидентов в критической информационной инфраструктуре;
- действия должностных лиц, персонала и владельцев АСУ КВО и иных объектов критической инф. инфраструктуры при обнаружении несанкционированного доступа к обрабатываемой информации и иных компьютерных инцидентах;
- ответственность за нарушение установленного порядка разработки, ввода в действие, эксплуатации и модернизации АСУ КВО и иных объектов критической информационной инфраструктуры;
- правовые основания и порядок применения мер принудительного изменения информационного обмена с объектами информатизации, являющимися источниками компьютерных атак, вплоть до полного его прекращения;

б) проведение паспортизации автоматизированных систем управления КВО;

в) реализацию первоочередных мероприятий, направленных на минимизацию прохождения информационного обмена между российскими абонентами по территориям иностранных государств;

г) разработку системы грантов для частных лиц и организаций, призванных стимулировать исследования в области обнаружения уязвимостей ПО и оборудования АСУ КВО и иных объектов критической информационной инфраструктуры;

д) разработку комплексных систем защиты и обеспечения безопасности АСУ КВО и иных объектов критической информационной инфраструктуры, отвечающих современному уровню развития информационных и коммуникационных технологий и минимизирующих участие обслуживающего персонала в настройке и эксплуатации входящих в их состав программно-аппаратных средств;

е) определение необходимых объемов и источников финансовых ресурсов (бюджетных и внебюджетных) на реализацию программ и планов мероприятий в области обеспечения безопасности АСУ КВО и критической информационной инфраструктуры в целом на последующих этапах реализации настоящих Основных направлений;

ж) ввод в эксплуатацию первой очереди Ситуационного центра единой государственной системы обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру и оценки уровня реальной защищенности ее элементов;

з) создание сил и средств ликвидации последствий компьютерных инцидентов в критической информационной инфраструктуре.

Основные направления государственной политики в области обеспечения безопасности АСУ производственными и технологическими процессами критически важных объектов инфраструктуры РФ (утв. Президентом РФ 03.02.2012 г. N 803)

19. На третьем этапе (2017 - 2020 годы) необходимо осуществить:

а) внедрение комплексных систем защиты и обеспечения безопасности автоматизированных систем управления КВО и иных объектов критической информационной инфраструктуры, отвечающих современному уровню развития информационных технологий и минимизирующих участие обслуживающего персонала в настройке и эксплуатации входящих в их состав программно-аппаратных средств;

б) реализацию комплекса организационных, правовых, экономических и научно-технических мер по прекращению прохождения информационного обмена между российскими абонентами по территориям иностранных государств;

в) ввод в действие первой очереди хранилища эталонного программного обеспечения, используемого в автоматизированных системах управления КВО и на других объектах критической информационной инфраструктуры;

г) внедрение системы грантов для частных лиц и организаций для стимулирования исследований в области обнаружения уязвимостей программного обеспечения и оборудования автоматизированных систем управления КВО и иных объектов критической информационной инфраструктуры;

д) ввод в эксплуатацию Ситуационного центра единой государственной системы обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру Российской Федерации и оценки уровня реальной защищенности ее элементов и ситуационных центров регионального и ведомственного уровней;

е) создание для автоматизированных систем управления КВО специализированных экономически целесообразных информационных технологий, исключающих или в максимальной степени снижающих на технологическом уровне обмен информацией, подлежащей обязательной защите;

ж) ввод в эксплуатацию в целом единой государственной системы обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру и оценки уровня реальной защищенности ее элементов.

20. В период после 2020 года осуществляется комплекс мероприятий по поддержанию организационной, экономической, научно-технической и технологической готовности Российской Федерации к предотвращению угроз безопасности ее критической информационной инфраструктуры.

Основные направления государственной политики в области обеспечения безопасности АСУ производственными и технологическими процессами критически важных объектов инфраструктуры РФ (утв. Президентом РФ 03.02.2012 г. N 803)

Достоинства документа

Появление такого документа в рамках работы Совета безопасности говорит о признании всей серьезности киберугроз и их возможном негативном (и даже разрушительном) влиянии на критически важную инфраструктуру страны. В данном вопросе этот документ соответствует международной практике по защите собственных интересов в киберпространстве и определении потенциально уязвимых точек, которые могут стать мишенью для кибертеррористов или кибервандалов. Международный опыт показывает, что развитые страны уделяют этому вопросу большое значение и предпринимают шаги по защите собственной инфраструктуры от интернет-угроз.

Очень важным является предусмотренное документом создание единой государственной системы обнаружения и предупреждения компьютерных атак на критическую информационную инфраструктуру и оценки уровня реальной защищенности ее элементов.

К другим достоинствам документа можно отнести выдвижение требований к разработчикам систем АСУ и введение ответственности за нарушение порядка их разработки, что является некоторым ноу-хау для наших регуляторов, ранее не сильно озабоченных требованиями к разработчикам прикладного ПО, однако, учитывая, что большинство наших АСУ – зарубежного производства, не ясен порядок реализации этого требования.

Недостатки документа

Среди проблемных мест документа можно отметить отсутствие исчерпывающего перечня критически важных объектов инфраструктуры и объектов повышенной опасности в России. Что делать – определяется, а кому – пока не ясно.

Не ясен и механизм предусмотренного документом недопущения технологической или иной зависимости от иностранных государств при осуществлении деятельности в области обеспечения безопасности АСУ критически важных объектов в условиях, когда большинство используемых в России систем АСУ ТП (SCADA) – зарубежного производства.

Кроме того, в документе отсутствуют упоминания о ФСТЭК России. Фактически все функции реализации программы возлагаются на ФСБ, в зоне ответственности которой ранее были только криптографические средства защиты и информационная безопасность высших органов власти. Между тем, реализация «Основных направлений...» политики требует принятия большого количества нормативно-правовых актов, часть которых, в соответствии с действующими документами, входит в компетенцию ФСТЭК.

«Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», утвержденная Президентом РФ 12.12.2014 № К 1274
(выписка, источник <http://www.consultant.ru>)

...

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.

...

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;

...

**«Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», утвержденная Президентом РФ 12.12.2014 № К 1274
(выписка, источник <http://www.consultant.ru>)**

7. Продолжение

...

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.

Федеральный закон от 26 июля 2017 г. N 187-ФЗ

"О безопасности критической информационной инфраструктуры РФ"

Статья 1. Сфера действия настоящего Федерального закона

Настоящий **Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации** (далее также - критическая информационная инфраструктура) **в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.**

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

...

2) **безопасность критической информационной инфраструктуры** - состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак;

3) **значимый объект критической информационной инфраструктуры** - объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры;

4) **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;

5) **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;

6) **критическая информационная инфраструктура** - объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов;

7) **объекты критической информационной инфраструктуры** - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры;

8) **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, топливно-энергетического 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.

"О безопасности критической информационной инфраструктуры РФ"

Статья 4. Принципы обеспечения безопасности критической информационной инфраструктуры

Принципами обеспечения безопасности критической информационной инфраструктуры являются:

1) законность;

2) непрерывность и комплексность обеспечения безопасности критической информационной инфраструктуры, достигаемые в том числе за счет взаимодействия уполномоченных федеральных органов исполнительной власти и субъектов критической информационной инфраструктуры;

3) приоритет предотвращения компьютерных атак.

"О безопасности критической информационной инфраструктуры РФ"

Статья 5. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

1. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ представляет собой единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. В целях настоящей статьи под информационными ресурсами РФ понимаются информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, находящиеся на территории РФ, в дипломатических представительствах и (или) консульских учреждениях РФ.

2. К силам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, относятся:

1) подразделения и должностные лица федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

2) организация, создаваемая федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, для обеспечения координации деятельности субъектов критической информационной инфраструктуры по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты (далее - **национальный координационный центр по компьютерным инцидентам**);

3) подразделения и должностные лица субъектов критической информационной инфраструктуры, которые принимают участие в обнаружении, предупреждении и ликвидации последствий компьютерных атак и в реагировании на компьютерные инциденты.

3. Средствами, предназначенными для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, являются технические, программные, программно-аппаратные и иные средства для обнаружения (в том числе для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры), предупреждения, ликвидации последствий компьютерных атак и (или) обмена информацией, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак, а также криптографические средства защиты такой информации.

"О безопасности критической информационной инфраструктуры РФ"

Статья 5. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (продолжение)

4. Национальный координационный центр по компьютерным инцидентам осуществляет свою деятельность в соответствии с положением, утверждаемым федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ.

5. В государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации осуществляются сбор, накопление, систематизация и анализ информации, которая поступает в данную систему через средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак, информации, которая представляется субъектами критической информационной инфраструктуры и федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, в соответствии с перечнем информации и в порядке, определяемыми федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также информации, которая может представляться иными не являющимися субъектами критической информационной инфраструктуры органами и организациями, в том числе иностранными и международными.

6. Федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, организует в установленном им порядке обмен информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры, а также между субъектами критической информационной инфраструктуры и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты.

7. Предоставление из государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ сведений, составляющих государственную либо иную охраняемую законом тайну, осуществляется в соответствии с законодательством РФ.

"О безопасности критической информационной инфраструктуры РФ"

Статья 7. Категорирование объектов критической информационной инфраструктуры

1. Категорирование объекта критической информационной инфраструктуры представляет собой установление соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения.

2. Категорирование осуществляется исходя из:

1) социальной значимости, выражающейся в оценке возможного ущерба, причиняемого жизни или здоровью людей, возможности прекращения или нарушения функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, а также максимальном времени отсутствия доступа к государственной услуге для получателей такой услуги;

2) политической значимости, выражающейся в оценке возможного причинения ущерба интересам Российской Федерации в вопросах внутренней и внешней политики;

3) экономической значимости, выражающейся в оценке возможного причинения прямого и косвенного ущерба субъектам критической информационной инфраструктуры и (или) бюджетам Российской Федерации;

4) экологической значимости, выражающейся в оценке уровня воздействия на окружающую среду;

5) значимости объекта критической информационной инфраструктуры для обеспечения обороны страны, безопасности государства и правопорядка.

3. Устанавливаются три категории значимости объектов критической информационной инфраструктуры - первая, вторая и третья.

4. Субъекты критической информационной инфраструктуры в соответствии с критериями значимости и показателями их значений, а также порядком осуществления категорирования присваивают одну из категорий значимости принадлежащим им на праве собственности, аренды или ином законном основании объектам критической информационной инфраструктуры. Если объект критической информационной инфраструктуры не соответствует критериям значимости, показателям этих критериев и их значениям, ему не присваивается ни одна из таких категорий.

5. Сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий субъекты критической информационной инфраструктуры в письменном виде в десятидневный срок со дня принятия ими соответствующего решения направляют в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, по утвержденной им форме.

"О безопасности критической информационной инфраструктуры РФ"

Статья 7. Категорирование объектов критической информационной инфраструктуры (продолжение)

6. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, в тридцатидневный срок со дня получения сведений, указанных в части 5 настоящей статьи, **проверяет соблюдение порядка осуществления категорирования и правильность присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо неприсвоения ему ни одной из таких категорий.**

7. **В случае, если субъектом критической информационной инфраструктуры соблюден порядок осуществления категорирования и принадлежащему ему на праве собственности, аренды или ином законном основании объекту критической информационной инфраструктуры правильно присвоена одна из категорий значимости, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, вносит сведения о таком объекте критической информационной инфраструктуры в реестр значимых объектов критической информационной инфраструктуры, о чем в десятидневный срок уведомляется субъект критической информационной инфраструктуры.**

8. **В случае, если федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, выявлены нарушения порядка осуществления категорирования и (или) объекту критической информационной инфраструктуры, принадлежащему на праве собственности, аренды или ином законном основании субъекту критической информационной инфраструктуры, неправильно присвоена одна из категорий значимости и (или) необоснованно не присвоена ни одна из таких категорий и (или) субъектом критической информационной инфраструктуры представлены неполные и (или) недостоверные сведения о результатах присвоения такому объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, в десятидневный срок со дня поступления представленных сведений возвращает их в письменном виде субъекту критической информационной инфраструктуры с мотивированным обоснованием причин возврата.**

"О безопасности критической информационной инфраструктуры РФ"

Статья 7. Категорирование объектов критической информационной инфраструктуры (продолжение)

9. **Субъект критической информационной инфраструктуры после получения мотивированного обоснования причин возврата сведений, указанных в части 5 настоящей статьи, не более чем в десятидневный срок устраняет отмеченные недостатки и повторно направляет такие сведения в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации.**

10. **Сведения об отсутствии необходимости присвоения объекту критической информационной инфраструктуры одной из категорий значимости после их проверки направляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры РФ, в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, о чем в десятидневный срок уведомляется субъект критической информационной инфраструктуры.**

11. В случае непредставления субъектом критической информационной инфраструктуры сведений, указанных в части 5 настоящей статьи, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, направляет в адрес указанного субъекта требование о необходимости соблюдения положений настоящей статьи.

12. **Категория значимости, к которой отнесен значимый объект критической информационной инфраструктуры, может быть изменена в порядке, предусмотренном для категорирования, в следующих случаях:**

1) по мотивированному решению федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, принятому по результатам проверки, проведенной в рамках осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры;

2) в случае изменения значимого объекта критической информационной инфраструктуры, в результате которого такой объект перестал соответствовать критериям значимости и показателям их значений, на основании которых ему была присвоена определенная категория значимости;

3) в связи с ликвидацией, реорганизацией субъекта критической информационной инфраструктуры и (или) изменением его организационно-правовой формы, в результате которых были изменены либо утрачены признаки субъекта критической информационной инфраструктуры.

"О безопасности критической информационной инфраструктуры РФ"

Статья 8. Реестр значимых объектов критической информационной инфраструктуры

1. В целях учета значимых объектов критической информационной инфраструктуры федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, ведет реестр значимых объектов критической информационной инфраструктуры в установленном им порядке. В данный реестр вносятся следующие сведения:

- 1) наименование значимого объекта критической информационной инфраструктуры;
- 2) наименование субъекта критической информационной инфраструктуры;
- 3) сведения о взаимодействии значимого объекта критической информационной инфраструктуры и сетей электросвязи;
- 4) сведения о лице, эксплуатирующем значимый объект критической информационной инфраструктуры;
- 5) категория значимости, которая присвоена значимому объекту критической информационной инфраструктуры;
- 6) сведения о программных и программно-аппаратных средствах, используемых на значимом объекте критической информационной инфраструктуры;
- 7) меры, применяемые для обеспечения безопасности значимого объекта критической информационной инфраструктуры.

2. Сведения из реестра значимых объектов критической информационной инфраструктуры направляются в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

3. В случае утраты значимым объектом критической информационной инфраструктуры категории значимости он исключается федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, из реестра значимых объектов критической информационной инфраструктуры.

"О безопасности критической информационной инфраструктуры РФ"**Статья 9. Права и обязанности субъектов критической информационной инфраструктуры****1. Субъекты критической информационной инфраструктуры имеют право:**

1) получать от федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, информацию, необходимую для обеспечения безопасности значимых объектов критической информационной инфраструктуры, принадлежащих им на праве собственности, аренды или ином законном основании, в том числе об угрозах безопасности обрабатываемой такими объектами информации и уязвимости программного обеспечения, оборудования и технологий, используемых на таких объектах;

2) в порядке, установленном федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, получать от указанного органа информацию о средствах и способах проведения компьютерных атак, а также о методах их предупреждения и обнаружения;

3) при наличии согласия федерального органа исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, за свой счет приобретать, арендовать, устанавливать и обслуживать средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

4) разрабатывать и осуществлять мероприятия по обеспечению безопасности значимого объекта критической информационной инфраструктуры.

"О безопасности критической информационной инфраструктуры РФ"

Статья 9. Права и обязанности субъектов критической информационной инфраструктуры
(продолжение)

2. Субъекты критической информационной инфраструктуры обязаны:

1) незамедлительно информировать о компьютерных инцидентах федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также Центральный банк Российской Федерации (в случае, если субъект критической информационной инфраструктуры осуществляет деятельность в банковской сфере и в иных сферах финансового рынка) в установленном указанным федеральным органом исполнительной власти порядке (в банковской сфере и в иных сферах финансового рынка указанный порядок устанавливается по согласованию с Центральным банком Российской Федерации);

2) оказывать содействие должностным лицам федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов;

3) в случае установки на объектах критической информационной инфраструктуры средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, обеспечивать выполнение порядка, технических условий установки и эксплуатации таких средств, их сохранность.

"О безопасности критической информационной инфраструктуры РФ"

Статья 9. Права и обязанности субъектов критической информационной инфраструктуры (продолжение)

3. Субъекты критической информационной инфраструктуры, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, наряду с выполнением обязанностей, предусмотренных частью 2 настоящей статьи, **также обязаны:**

1) **соблюдать требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленные федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;**

2) **выполнять предписания должностных лиц федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, об устранении нарушений** в части соблюдения требований по обеспечению безопасности значимого объекта критической информационной инфраструктуры, выданные этими лицами в соответствии со своей компетенцией;

3) **реагировать на компьютерные инциденты в порядке, утвержденном федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, принимать меры по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры;**

4) **обеспечивать беспрепятственный доступ должностным лицам федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, к значимым объектам критической информационной инфраструктуры** при реализации этими лицами полномочий, предусмотренных статьей 13 настоящего Федерального закона.

"О безопасности критической информационной инфраструктуры РФ"**Статья 10. Система безопасности значимого объекта критической информационной инфраструктуры**

1. В целях обеспечения безопасности значимого объекта критической информационной инфраструктуры субъект критической информационной инфраструктуры в соответствии с требованиями к созданию систем безопасности таких объектов и обеспечению их функционирования, утвержденными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, создает систему безопасности такого объекта и обеспечивает ее функционирование.

2. Основными задачами системы безопасности значимого объекта критической информационной инфраструктуры являются:

1) предотвращение неправомерного доступа к информации, обрабатываемой значимым объектом критической информационной инфраструктуры, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;

2) недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта критической информационной инфраструктуры;

3) восстановление функционирования значимого объекта критической информационной инфраструктуры, обеспечиваемого в том числе за счет создания и хранения резервных копий необходимой для этого информации;

4) непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

"О безопасности критической информационной инфраструктуры РФ"

Статья 11. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры

1. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, устанавливаемые федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, дифференцируются в зависимости от категории значимости объектов критической информационной инфраструктуры и этими требованиями предусматриваются:

1) планирование, разработка, совершенствование и осуществление внедрения мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры;

2) принятие организационных и технических мер для обеспечения безопасности значимых объектов критической информационной инфраструктуры;

3) установление параметров и характеристик программных и программно-аппаратных средств, применяемых для обеспечения безопасности значимых объектов критической информационной инфраструктуры.

2. Государственные органы и российские юридические лица, выполняющие функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере деятельности, по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, могут устанавливать дополнительные требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, содержащие особенности функционирования таких объектов в установленной сфере деятельности.

"О безопасности критической информационной инфраструктуры РФ"

Статья 12. Оценка безопасности критической информационной инфраструктуры

1. **Оценка безопасности критической информационной инфраструктуры осуществляется федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, в целях прогнозирования возникновения возможных угроз безопасности критической информационной инфраструктуры и выработки мер по повышению устойчивости ее функционирования при проведении в отношении ее компьютерных атак.**

2. **При осуществлении оценки безопасности критической информационной инфраструктуры проводится анализ:**

1) **данных, получаемых при использовании средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, в том числе информации о наличии в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры, признаков компьютерных атак;**

2) **информации, представляемой субъектами критической информационной инфраструктуры и федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, в соответствии с перечнем информации и в порядке, определяемыми федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также иными не являющимися субъектами критической информационной инфраструктуры органами и организациями, в том числе иностранными и международными;**

3) **сведений, представляемых в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, о нарушении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, в результате которого создаются предпосылки возникновения компьютерных инцидентов;**

4) **иной информации, получаемой федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, в соответствии с законодательством Российской Федерации.**

"О безопасности критической информационной инфраструктуры РФ"**Статья 12. Оценка безопасности критической информационной инфраструктуры**
(продолжение)

3. Для реализации положений, предусмотренных частями 1 и 2 настоящей статьи, **федеральный орган исполнительной власти**, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, **организует установку в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры, средств, предназначенных для поиска признаков компьютерных атак в таких сетях электросвязи.**

4. **В целях разработки мер по совершенствованию безопасности критической информационной инфраструктуры федеральный орган исполнительной власти**, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, направляет в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации*, результаты осуществления оценки безопасности критической информационной инфраструктуры.

* ФСТЭК (Проект Указа Президента Российской Федерации "О федеральном органе исполнительной власти, уполномоченном в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации" (подготовлен ФСТЭК России 30.08.2017))

"О безопасности критической информационной инфраструктуры РФ"

Статья 13. Государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры

1. Государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры проводится в целях проверки соблюдения субъектами критической информационной инфраструктуры, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, **требований, установленных настоящим ФЗ и принятыми в соответствии с ним НПА. Указанный государственный контроль проводится путем осуществления федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры РФ, плановых или внеплановых проверок.**

2. Основанием для осуществления плановой проверки является истечение трех лет со дня:

- 1) внесения сведений об объекте критической информационной инфраструктуры в реестр значимых объектов критической информационной инфраструктуры;
- 2) окончания осуществления последней плановой проверки в отношении значимого объекта критической информационной инфраструктуры.

3. Основанием для осуществления внеплановой проверки является:

1) истечение срока выполнения субъектом критической информационной инфраструктуры выданного федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, предписания об устранении выявленного нарушения требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры;

2) возникновение компьютерного инцидента, повлекшего негативные последствия, на значимом объекте критической информационной инфраструктуры;

3) приказ (распоряжение) руководителя **ФОИБ**, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры РФ, изданный в соответствии с поручением Президента РФ или Правительства РФ **либо на основании требования прокурора об осуществлении внеплановой проверки в рамках проведения надзора за исполнением законов по поступившим в органы прокуратуры материалам и обращениям.**

4. По итогам плановой или внеплановой проверки федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, составляется акт проверки по утвержденной указанным органом форме.

5. На основании акта проверки в случае выявления нарушения требований настоящего Федерального закона и принятых в соответствии с ним нормативных правовых актов по обеспечению безопасности значимых объектов критической информационной инфраструктуры **ФОИБ**, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры РФ, **выдает субъекту критической информационной инфраструктуры предписание об устранении выявленного нарушения с указанием сроков его устранения.**

Указ Президента РФ от 16.08.2004 N 1085 (ред. от 08.05.2018) "Вопросы Федеральной службы по техническому и экспортному контролю" (Выписка)

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) является федеральным органом исполнительной власти, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности по вопросам:

- 1) обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура);
- 2) противодействия иностранным техническим разведкам на территории Российской Федерации (далее - противодействие техническим разведкам);
- 3) обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней на территории Российской Федерации (далее - техническая защита информации);
- 4) защиты информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств;
- 5) осуществления экспортного контроля.

2. **ФСТЭК России является федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, а также специально уполномоченным органом в области экспортного контроля.**

ФСТЭК России является органом защиты государственной тайны, наделенным полномочиями по распоряжению сведениями, составляющими государственную тайну.

ФСТЭК России организует деятельность государственной системы противодействия техническим разведкам и технической защиты информации и руководит ею.

Руководство деятельностью ФСТЭК России осуществляет Президент Российской Федерации.

3. ФСТЭК России подведомственна Минобороны России.

Указ президента РФ от 15.01.2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»

ВЫПИСКА (источник <http://www.kremlin.ru/acts/bank/36691>)

В целях обеспечения информационной безопасности Российской Федерации постановляю:

1. Возложить на Федеральную службу безопасности Российской Федерации полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации - информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом.

2. Определить основными задачами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации:

а) прогнозирование ситуации в области обеспечения информационной безопасности Российской Федерации;

б) обеспечение взаимодействия владельцев информационных ресурсов Российской Федерации, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак;

в) осуществление контроля степени защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак;

г) установление причин компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации.

Указ президента РФ от 15.01.2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»

3. Установить, что Федеральная служба безопасности Российской Федерации:

а) организует и проводит работы по созданию государственной системы, названной в пункте 1 настоящего Указа, осуществляет контроль за исполнением этих работ, а также обеспечивает во взаимодействии с государственными органами функционирование ее элементов;

б) разрабатывает методику обнаружения компьютерных атак на информационные системы и информационно-телекоммуникационные сети государственных органов и по согласованию с их владельцами - на иные информационные системы и информационно-телекоммуникационные сети;

в) определяет порядок обмена информацией между федеральными органами исполнительной власти о компьютерных инцидентах, связанных с функционированием информационных ресурсов Российской Федерации;

г) организует и проводит в соответствии с законодательством Российской Федерации мероприятия по оценке степени защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак;

д) разрабатывает методические рекомендации по организации защиты критической информационной инфраструктуры Российской Федерации от компьютерных атак;

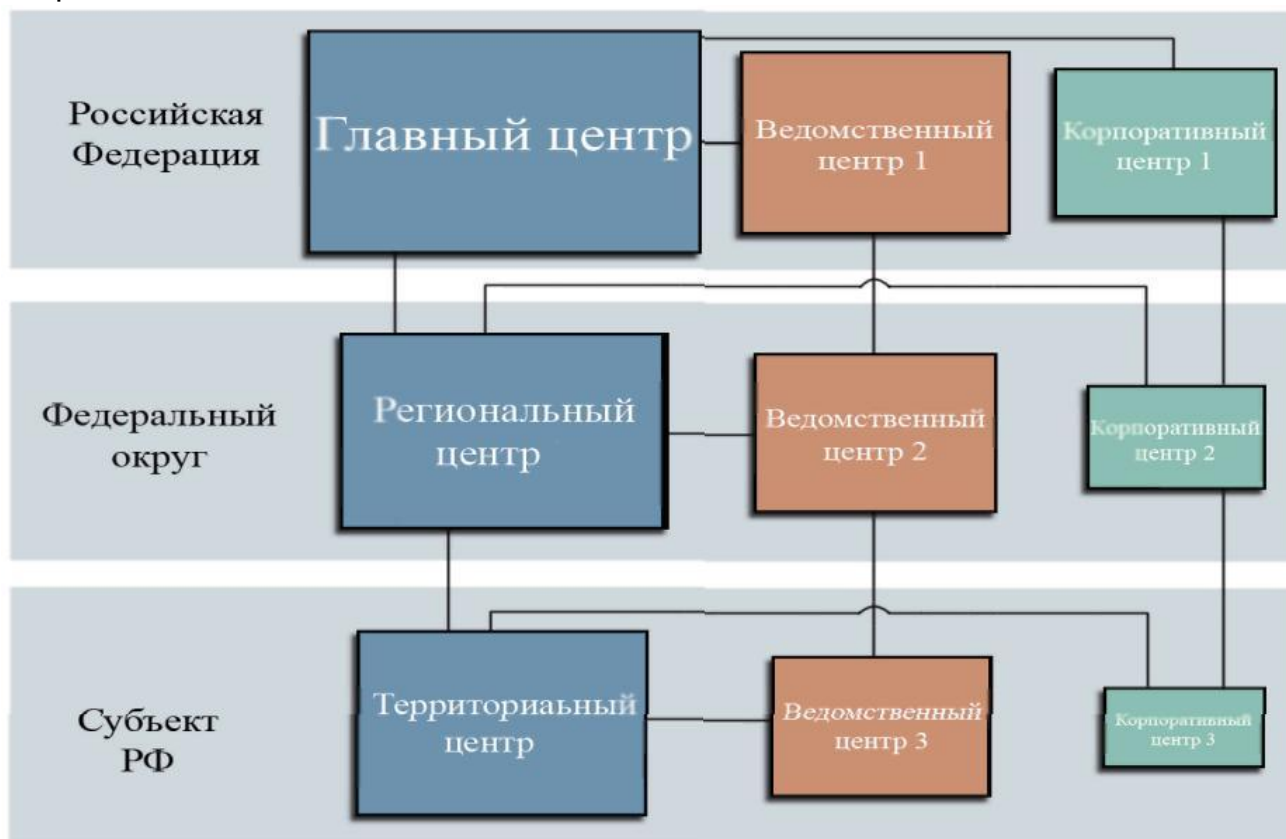
е) определяет порядок обмена информацией между федеральными органами исполнительной власти и уполномоченными органами иностранных государств (международными организациями) о компьютерных инцидентах, связанных с функционированием информационных ресурсов, и организует обмен такой информацией.

4. Настоящий Указ вступает в силу со дня его подписания.

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ

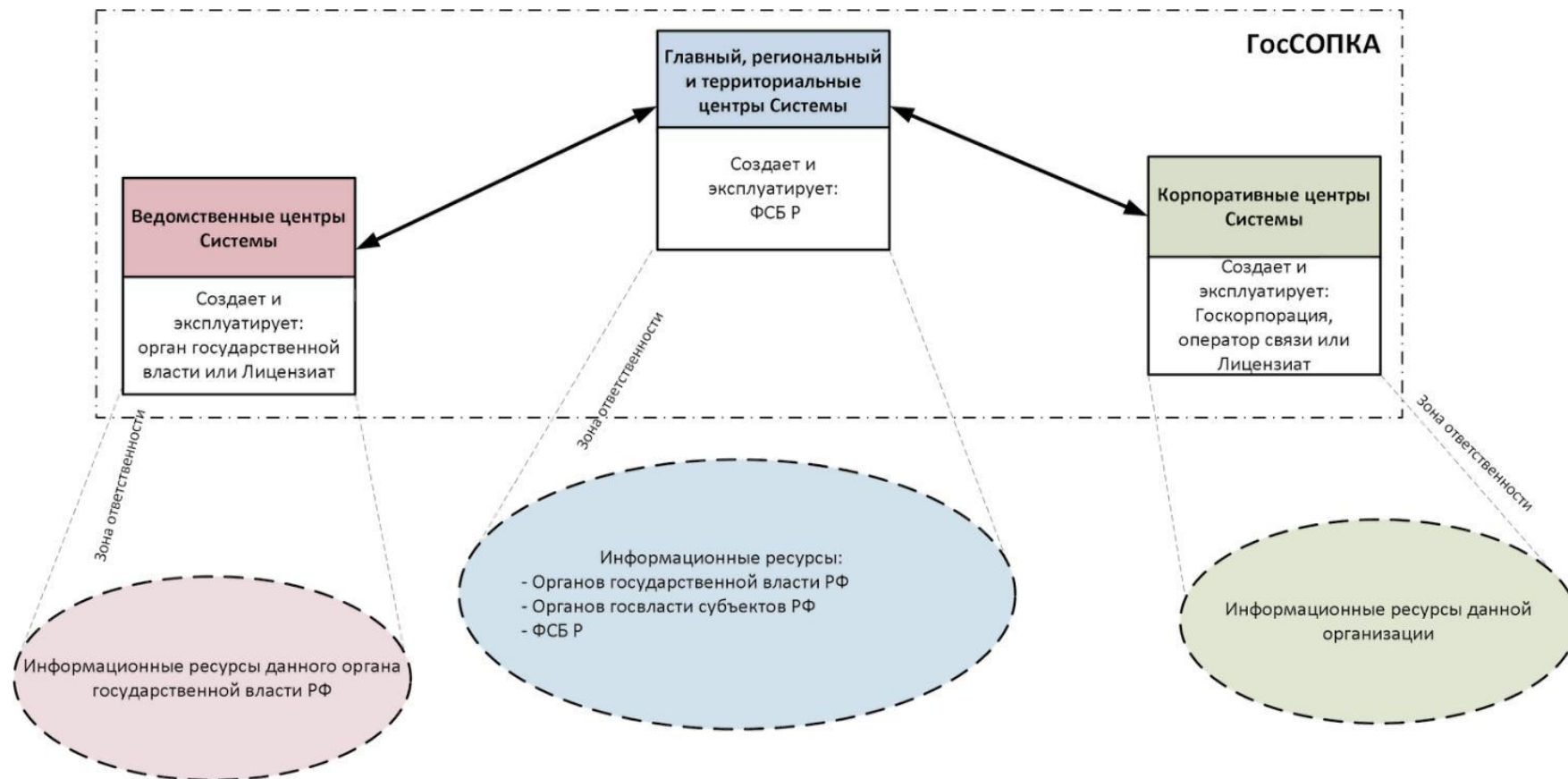
В соответствии с концепцией территориальная структура ГосСОПКА имеет вид, представленный ниже.

Архитектурно она представляет собой единый территориально распределенный комплекс центров различного масштаба, обменивающихся информацией о кибератаках. Такие центры обязаны создать все компании, которым принадлежат объекты критической информационной инфраструктуры (такие компании называют субъектами КИИ). Цель всей этой масштабной государственной инициативы – создать между важнейшими организациями страны систему обмена информацией о ведущихся кибератаках и тем самым обеспечить возможность превентивной защиты.



Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

Область ответственности центров ГосСОПКА отображена на следующей схеме:



Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

Сертифицированные последнее время в ФСБ средства обнаружения компьютерных атак должны иметь возможность интеграции с ГосСОПКА. В требованиях по созданию ГИС в последнее время также указывается необходимость применения систем обнаружения вторжений (COB) с возможностью интеграции с ГосСОПКА.

Таким образом, можно предположить что в качестве так называемых “технических средств, предназначенные для поиска признаков компьютерных атак в сообщениях электросвязи” будет выступать любое сертифицированное в ФСБ IPS, которое будет опрашивать информацию об атаках и инцидентах в специальном формате, а ГосСОПКА представляет из себя в таком случае большой распределенный SOC**.

С учетом этого, а также функций приведенных в Концепции, получается следующая схема взаимодействия ГосСОПКА

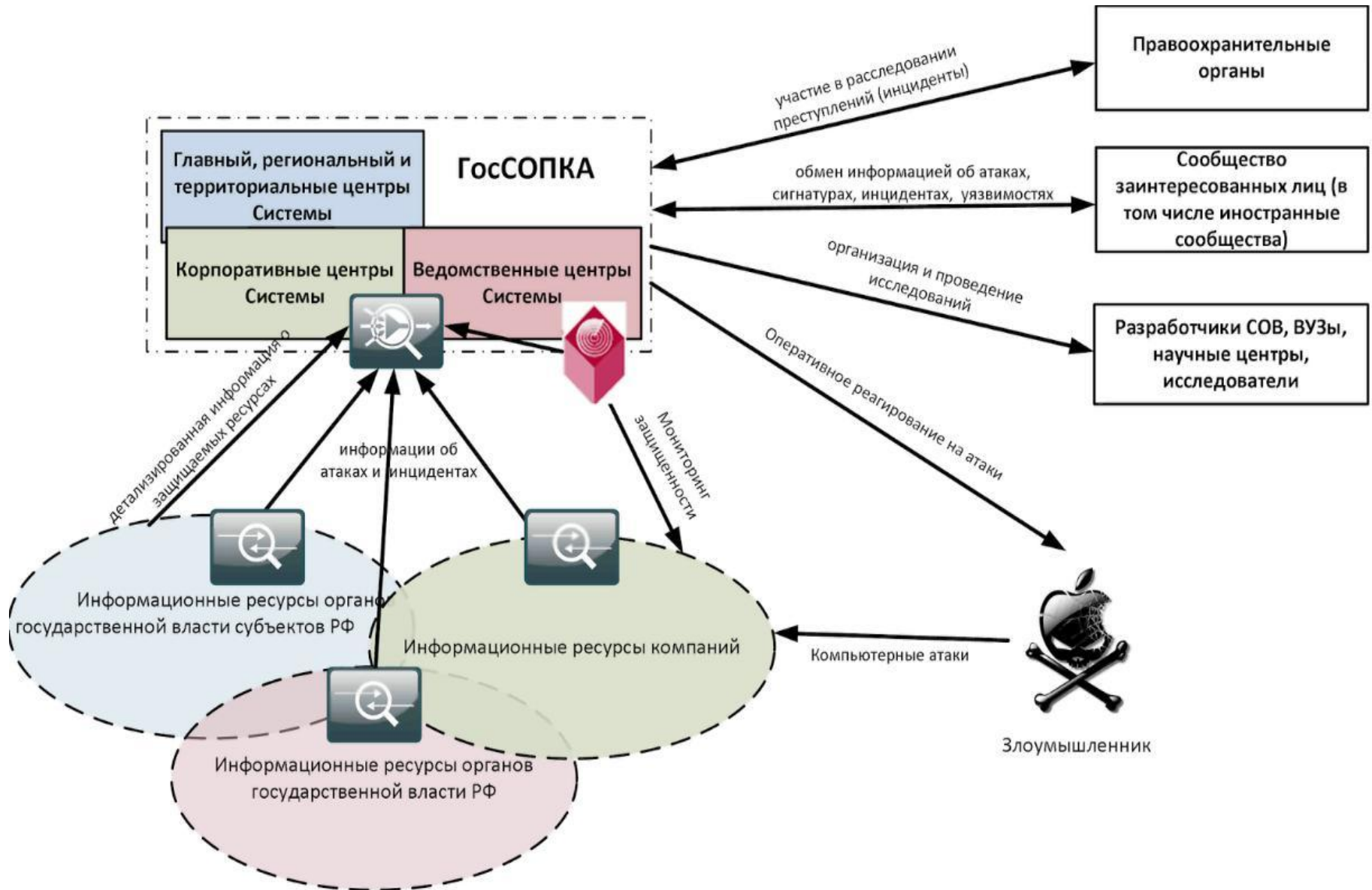
Примечание автора:

* IDS (Intrusion Detection System) – система обнаружения вторжений (COB). Программное или аппаратное средство, предназначенное для выявления фактов несанкционированного доступа (вторжения или сетевой атаки) в компьютерную систему или сеть;

IPS (Intrusion Prevention System) – система предотвращения вторжений. Программное или аппаратное средство, которое осуществляет мониторинг сети или компьютерной системы в реальном времени с целью выявления, предотвращения или блокировки вредоносной активности.

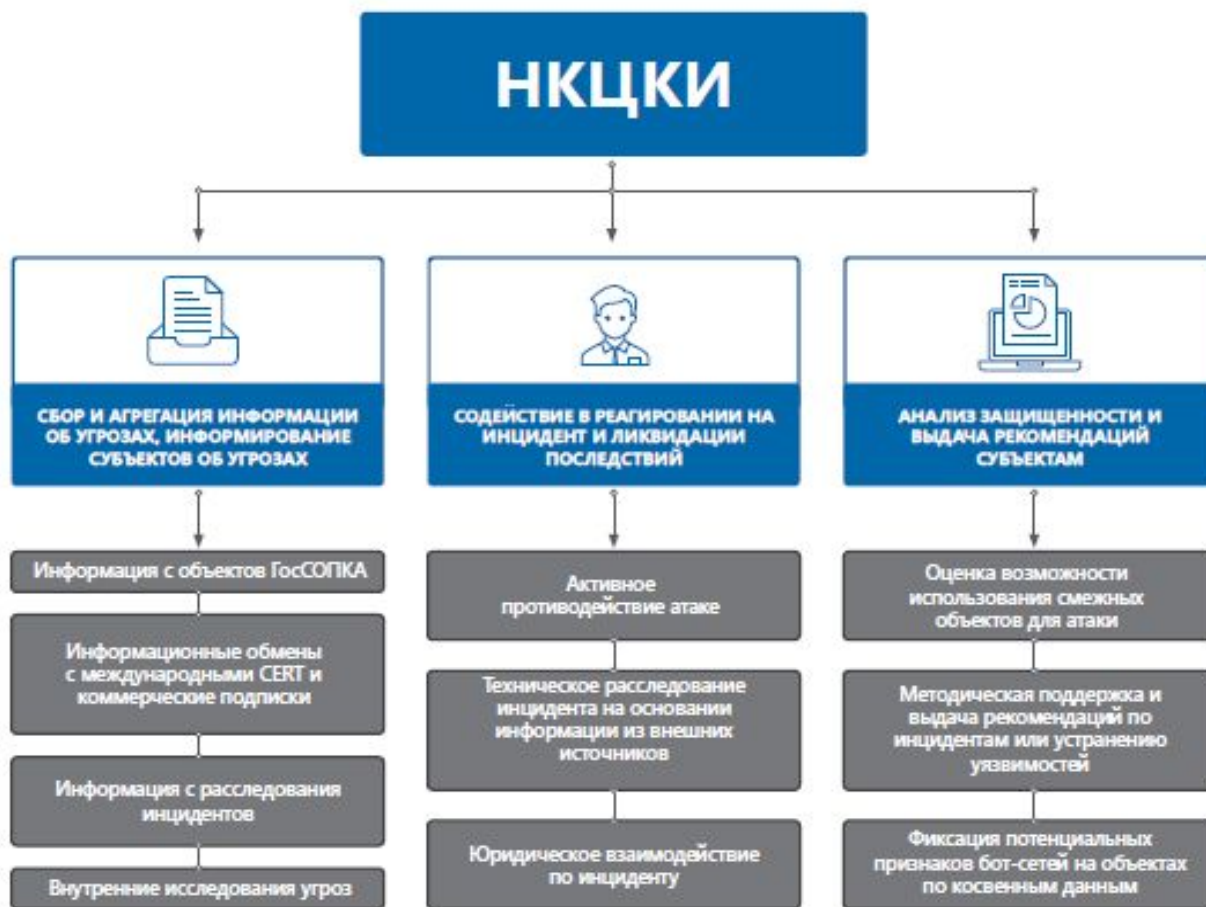
** SOC (Security Operation Center) – ситуационный центр информационной безопасности (центр мониторинга и реагирования на инциденты информационной безопасности).

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации



Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ

Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак является территориально распределенной совокупностью центров (сил и средств), организованной по ведомственному и территориальному принципам, в числе которых — Национальный координационный центр по компьютерным инцидентам.



Структура и схема функционирования НКЦКИ

Таким образом, НКЦКИ выступает в роли огромного информационного хаба и источника знаний о новых и актуальных угрозах безопасности информации (Threat Intelligence), которая может стать востребованной любым из участников информационного обмена в ГосСОПКА. И предоставляемая информация носит именно практический характер защиты от новых угроз и повышения защищенности конкретного объекта.

Модель построения ГосСОПКА, в которой ключевыми элементами системы являются ведомственные и корпоративные центры, призвана объединить специалистов реагирования и расследования компьютерных инцидентов в единое экспертное сообщество, обменивающегося обезличенной, но технически ценной информацией об угрозах безопасности. И это, с одной стороны, повышает ценность вклада каждого отдельного участника взаимодействия в обеспечение общей безопасности всех объектов КИИ, с другой стороны — позволяет рассчитывать на помощь «собратьев по оружию» и регулятора в отражении сложных и динамически развивающихся атак.

Проект Приказа ФСБ России "Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты"
(подготовлен ФСБ России 08.02.2018)

В документе обозначены пять основных подсистем центра ГосСОПКА:

технические, программные, программно-аппаратные и иные средства для обнаружения компьютерных атак (далее - средства обнаружения);

технические, программные, программно-аппаратные и иные средства для предупреждения компьютерных атак (далее - средства предупреждения);

технические, программные, программно-аппаратные и иные средства для ликвидации последствий компьютерных атак (далее - средства ликвидации последствий);

технические, программные, программно-аппаратные и иные средства поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ (далее - средства ППКА);

технические, программные, программно-аппаратные и иные средства обмена информацией, необходимой субъектам КИИ при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак (далее - средства обмена);

криптографические средства защиты информации, необходимой субъектам КИИ при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак.

Что такое «критическая информационная инфраструктура»?

Критическая информационная инфраструктура — объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов

Что такое объекты и субъекты КИИ?

Объекты критической информационной инфраструктуры — информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры

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, топливно-энергетического 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.

На кого возложены обязанности ГосСОПКА?

подразделения и должностные лица федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

организация, создаваемая федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, для обеспечения координации деятельности субъектов критической информационной инфраструктуры по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты (далее — национальный координационный центр по компьютерным инцидентам);

подразделения и должностные лица субъектов критической информационной инфраструктуры, которые принимают участие в обнаружении, предупреждении и ликвидации последствий компьютерных атак и в реагировании на компьютерные инциденты.

Какие действия должны предпринять субъекты КИИ для выполнения ФЗ-187?

провести категорирование объектов КИИ
обеспечить интеграцию (встраивание) в Государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА)
принять организационные и технические меры по обеспечению безопасности объектов КИИ

Что такое категорирование объектов КИИ?

Категорирование объекта критической информационной инфраструктуры представляет собой установление соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения.

Что такое значимый объект КИИ?

значимый объект критической информационной инфраструктуры — объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры.

Какие существуют категории значимости?

- социальная значимость, выражающаяся в оценке возможного ущерба, причиняемого жизни или здоровью людей, возможности прекращения или нарушения функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, а также максимальном времени отсутствия доступа к государственной услуге для получателей такой услуги;
- политическая значимость, выражающаяся в оценке возможного причинения ущерба интересам Российской Федерации в вопросах внутренней и внешней политики;
- экономическая значимость, выражающаяся в оценке возможного причинения прямого и косвенного ущерба субъектам критической информационной инфраструктуры и (или) бюджетам Российской Федерации;
- экологическая значимость, выражающаяся в оценке уровня воздействия на окружающую среду;
- значимость объекта критической информационной инфраструктуры для обеспечения обороны страны, безопасности государства и правопорядка.

Сколько категорий значимости установлено?

Устанавливаются три категории значимости объектов критической информационной инфраструктуры — первая, вторая и третья.

Если объект критической информационной инфраструктуры не соответствует критериям значимости, показателям этих критериев и их значениям, ему не присваивается ни одна из таких категорий.

Ответственность за невыполнение требований ФЗ-187

В УК РФ была добавлена новая статья 274.1, которая устанавливает уголовную ответственность должностных лиц субъекта КИИ за несоблюдение установленных правил эксплуатации технических средств объекта КИИ или нарушение порядка доступа к ним вплоть до лишения свободы сроком на 6 лет. Пока данная статья не предусматривает ответственности за невыполнение необходимых мероприятий по обеспечению безопасности объекта КИИ, однако в случае наступления последствий (аварий и чрезвычайных ситуаций, повлекших за собой крупный ущерб) непринятие таких мер подпадает по состав 293 статьи УК РФ «Халатность». Дополнительно следует ожидать внесения изменений в административное законодательство в части определения штрафных санкций для юридических лиц за неисполнение Закона. На сегодняшний день с высокой долей уверенности можно говорить о том, что именно введение существенных денежных штрафов будет стимулировать субъекты КИИ к выполнению требований Закона.

Источник: <http://gossopka.ru>

Вопрос 3

Центры реагирования на компьютерные инциденты в РФ

Центры реагирования на компьютерные инциденты

Компьютерная группа реагирования на чрезвычайные ситуации (англ. Computer Emergency Response Team, **CERT**), другие названия: **Команда компьютерной безопасности по реагированию на инциденты** (англ. Computer Security Incident Response Team, **CSIRT**), или **Компьютерная команда экстренной готовности** (англ. Computer Emergency Readiness Team) — названия экспертных групп, которые занимаются инцидентами в компьютерной и интернет-безопасности.

Название CERT является историческим обозначением первой группы в университете Карнеги — Меллон.

Университет Карнеги — Меллон (англ. Carnegie Mellon University, CMU) — частный университет и исследовательский центр, расположенный в Питтсбурге, (штат Пенсильвания, США). Университет занимается исследованиями в области науки и техники, инноваций в областях IT-технологий, робототехники и искусственного интеллекта. Университет также известен во многих других областях, включая менеджмент, экономику и лингвистику. Имеет партнёрские отношения с IBM и другими известными компаниями.

Университет имеет филиал в Катаре, совместные проекты в нескольких странах мира, включая центр подготовки IT-кадров в университете Иннополис в новом наукограде Иннополис в Татарстане.

Образование в области компьютерных технологий, конструирования, бизнеса и экономики, государственной службы, информационных систем, психологии, развлекательных технологий, социальных и управленческих наук (decision science) и искусств считается одним из лучших.

В 2010 году Университет в рейтинге US News and World Report занял 23 место, в рейтинге журнала Times Higher Education — 20 и 34 в мировом QS World University Rankings. Университет считается лучшим в подготовке специалистов в области компьютерных технологий.

Центры реагирования на компьютерные инциденты в РФ

Аббревиатуру CERT подхватили другие команды во всём мире. В англоязычных странах мира некоторые команды взяли название CSIRT.

История CERT тесно связана с борьбой против сетевых червей. Первый червь попал в сеть Интернета 3 ноября 1988 года, когда так называемый червь Морриса парализовал работу интернет-узлов. Это привело к формированию первого Computer Emergency Response Team в университете Карнеги — Меллон по контракту правительства США.

«CERT» является защищенным международным законодательством об авторских и патентных правах наименованием сервиса, зарегистрированным Университетом Карнеги, который имеет исключительное право на предоставление этого именованя различным сервисам информационной безопасности по всем миру.

Чтобы использовать торговую марку CERT необходимо получить соответствующее разрешение, которое в России получил только CERT-GIB.

Червь Морриса (Morris worm)

2 ноября 1988 года сеть ARPANET была атакована программой, впоследствии получившей название «червь Морриса» — по имени его создателя, студента Корнельского университета Роберта Морриса-младшего.

Сеть ARPANET (Advanced Research Projects Agency Network) была создана в 1969 году по инициативе Управления перспективных исследований Министерства Обороны США (DARPA, Defense Advanced Research Projects Agency) и явившаяся прототипом сети Интернет. Эта сеть создавалась в интересах исследователей в области вычислительной техники и технологии для обмена сообщениями, а также программами и массивами данных между крупнейшими исследовательскими центрами, лабораториями, университетами, государственными организациями и частными фирмами, выполняющими работы в интересах Министерства Обороны США (DoD, Department of Defense of USA). Именно по заказу DoD был разработан один из трех наиболее распространенных протоколов транспортного уровня модели OSI, получивший название TCP/IP, который в 1983 году стал основным в ARPANET. К концу 80-х годов сеть насчитывала несколько десятков тысяч ЭВМ. ARPANET прекратила своё существование в июне 1990 года.

«Червь Морриса» был первым в истории развития вычислительной техники образцом вредоносного программного обеспечения, который использовал механизмы автоматического распространения по сети. Для этого использовались несколько уязвимостей сетевых сервисов, а так же некоторые слабые места компьютерных систем, обусловленные недостаточным вниманием к вопросам безопасности в то время.

Червь Морриса (Morris worm)

По словам Роберта Морриса, червь был создан в исследовательских целях. Его код не содержал в себе никакой «полезной» нагрузки (деструктивных функций). Тем не менее, из-за допущенных ошибок в алгоритмах работы, распространение червя спровоцировало так называемый «отказ в обслуживании», когда ЭВМ были заняты выполнением многочисленных копий червя и переставали реагировать на команды операторов.

«Червь Морриса» практически парализовал работу компьютеров в сети ARPANET на срок до пяти суток.

Оценка простая — минимум 8 миллионов часов и свыше 1 миллиона часов временных затрат на восстановление работоспособности систем. Общие убытки в денежном эквиваленте оценивались в 98 миллионов долларов, они складывались из прямых и косвенных потерь.

К прямым потерям относились (32 миллиона долларов):

- остановка, тестирование и перезагрузка 42700 машин;
- идентификация червя, удаление, чистка памяти и восстановление работоспособности 6200 машин;
- анализ кода червя, дизассемблирование и документирование;
- исправление UNIX-систем и тестирование.

К косвенным потерям были отнесены (66 миллионов долларов):

- потери машинного времени в результате отсутствия доступа к сети;
- потери доступа пользователей к сети.

Червь Морриса (Morris worm)

Структурно червь состоял из трех частей — «головы» и двух «хвостов». «Голова» представляла собой исходный текст на языке C (99 строк) и компилировалась непосредственно на удаленной машине. «Хвосты» были идентичными, с точки зрения исходного кода и алгоритмов, бинарными файлами, но скомпилированными под разные типы архитектур. По замыслу Морриса в качестве целевых аппаратных платформ были выбраны VAX и SUN. «Голова» забрасывалась при помощи следующих методов:

- использование отладочного режима в sendmail;
- использование уязвимости типа «переполнение буфера» в сетевом сервисе fingerd;
- подбор логина и пароля для удаленного выполнения программ (rexec);
- вызов удаленного командного интерпретатора (rsh) путем подбора логина и пароля или используя механизм доверия.

Для использования метода распространения через rexec и rsh собирался список пользователей локальной машины. На его основе производился подбор наиболее часто используемых паролей, в надежде что многие пользователи имеют одинаковые имена и пароли на всех машинах в сети, что впрочем оказалось недалеким от истины. Помимо подбора в rsh использовался механизм доверия, или по другому механизм упрощенной аутентификации по IP адресу удаленной машины. Такие адреса хранились в файлах /etc/hosts.equiv и .rhosts. Для большинства компьютеров доверие было взаимным, так что с большой долей вероятности, перечень IP адресов из этих файлов, найденных червем, позволял осуществить вход в удаленную систему через rsh вообще не используя пароль

При подборе червь пробовал следующие варианты паролей: пустой; имя пользователя (user); имя пользователя, написанное наоборот (resu); двойной повтор имени пользователя (useruser); имя или фамилия пользователя (John, Smith); имя или фамилия пользователя в нижнем регистре (john, smith); встроенный словарь размером 432 слова.

Червь Морриса (Morris worm)

Червь использовал несколько приемов для затруднения своего обнаружения администраторами компьютеров:

- удаление своего исполняемого файла после запуска;
- отключались все сообщения об ошибках, а размер аварийного дампа устанавливался в ноль;
- исполняемый файл червя сохранялся под именем sh, такое же имя использовалось командным интерпретатором Bourne Shell, таким образом, червь маскировался в списке процессов;
- примерно каждые три минуты порождался дочерний поток, а родительский завершался, при этом происходило постоянное изменение pid процесса червя и обнулялось время работы, показываемое в списке процессов;
- все текстовые строки были закодированы.

Червь имел в себе некоторые ошибки, как проектирования, так и реализации. Неправильно реализованный алгоритм проверки, не является ли система уже зараженной, привел к массовому распространению червя в сети, вопреки задумке его автора. На практике, компьютеры заражались многократно, что, во-первых, приводило к быстрому исчерпанию ресурсов, во-вторых — способствовало лавинообразному распространению червя в сети. По некоторым оценкам червь Морриса инфицировал порядка 6200 компьютеров. Сам разработчик, осознав масштабы результатов своего поступка, добровольно сдался властям и обо всем рассказал. Слушанье по его делу закончилось 22 января 1990 года. Изначально Моррису грозило до пяти лет лишения свободы и штраф в размере 25 тысяч долларов. В действительности приговор был достаточно мягок, суд назначил 400 часов общественных работ, 10 тысяч долларов штрафа, испытательный срок в три года и оплату расходов, связанных с наблюдением за осужденным.

Червь Морриса (Morris worm)

Инцидент с «червем Морриса» заставил специалистов в области IT серьезно задуматься о вопросах безопасности: после этого для повышения безопасности системы стало внедряться использование пауз после неправильного ввода пароля и хранение паролей в /etc/shadow (для Linux), куда они перенесены из доступного на чтение всем пользователям файла /etc/passwd.

Наиболее важным событием стало создание в ноябре 1988 года координационного центра CERT (CERT Coordination Center, CERT/CC), деятельность которого связана с решением проблем безопасности в Интернете. Первым появившимся в декабре 1988 года бюллетенем безопасности CERT стало сообщение об уязвимостях, использованных червем. Многие технические решения, используемые «червем Морриса», такие как использование перебора паролей, компиляция кода загрузчика на удаленной ЭВМ под управлением *NIX систем (Slapper), сканирование сети для выявления целей и т.д. применяются и в современных образцах вредоносного программного обеспечения.

В 1988 году, будучи под впечатлением от атаки червя Морриса, американская Ассоциация компьютерного оборудования объявила **30 ноября международным Днем защиты информации (Computer Security Day)**, который отмечается и по сей день.

Взаимодействие государства и бизнеса в области защиты критической информационной инфраструктуры

Определение SOC и CERT

Центр мониторинга информационной безопасности (SOC) –

это выделенное структурное подразделение, осуществляющее мониторинг и реагирование на инциденты информационной безопасности.

Computer Emergency Response Team (CERT) –

это централизованное подразделение или выделенная организация, основной деятельностью которой является информирование о новых угрозах ИБ и обмен.

Основные функции



Непрерывное выявление кибератак и инцидентов ИБ



Упреждающая реакция на новые уязвимости и угрозы ИБ



Быстрое устранение последствий инцидентов ИБ

Основные функции



Глубокий анализ и подробное исследование новых угроз



Информирование заинтересованных сторон

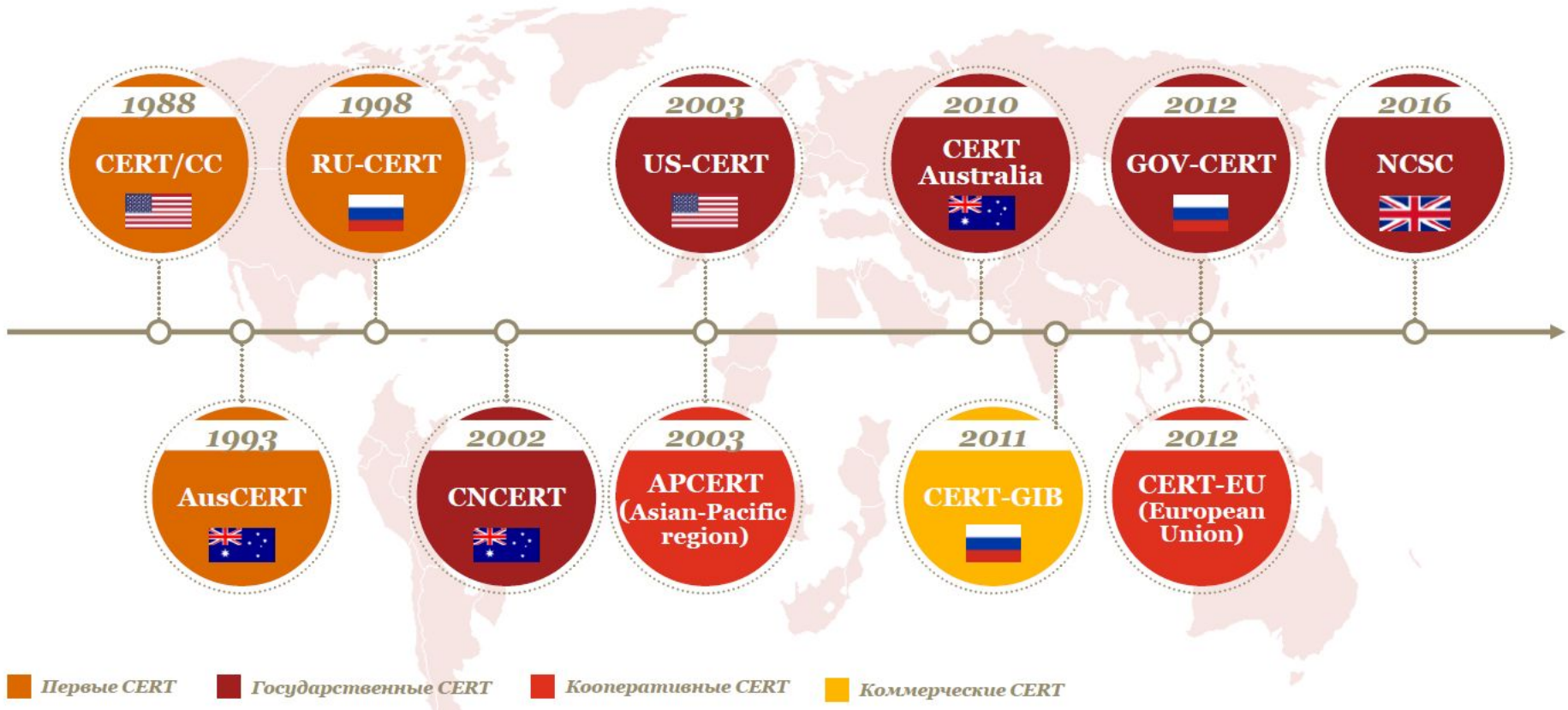


Координация и разработка инструкций по устранению уязвимостей

Ростелеком — не только один из крупнейших операторов связи, но и провайдер сервисов кибербезопасности (Managed Security Service Provider, MSSP)

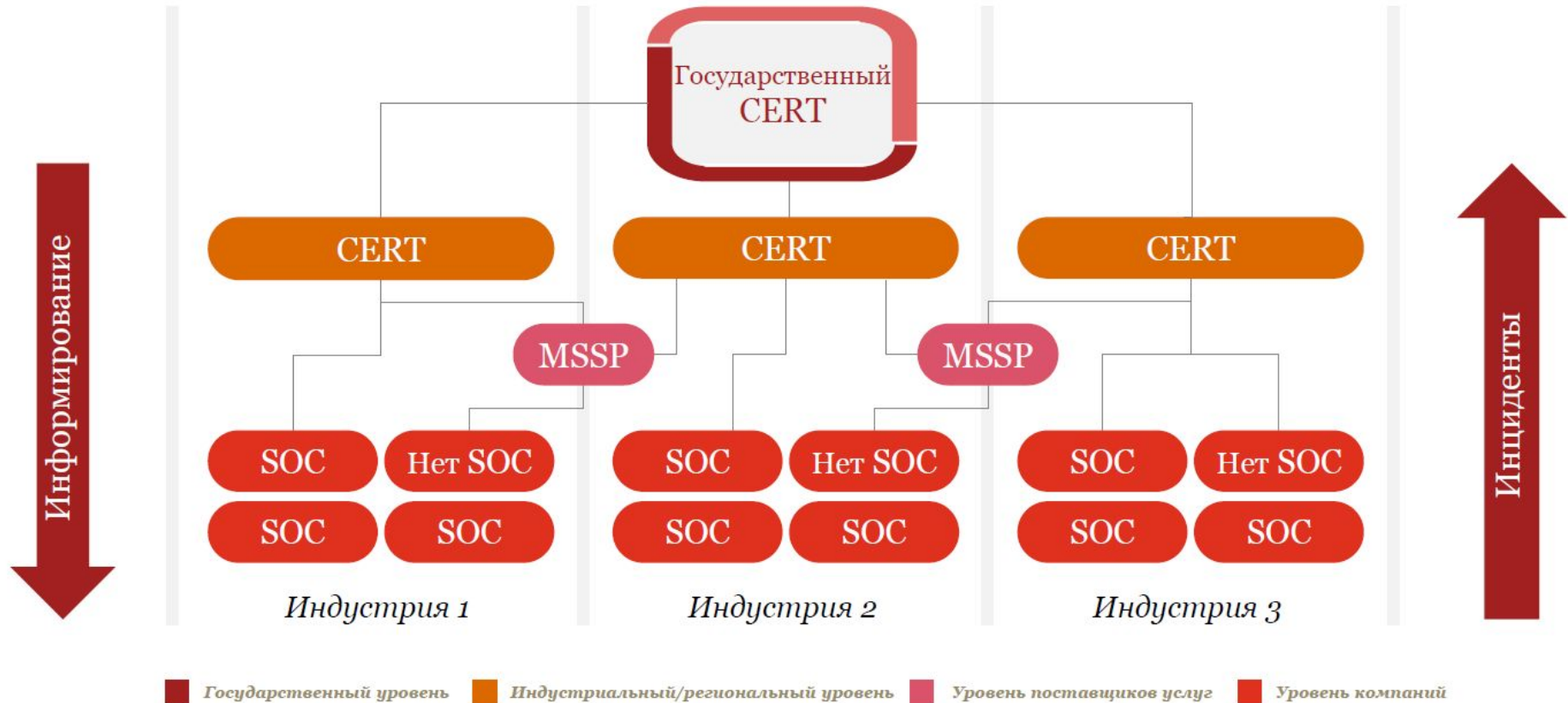
Взаимодействие государства и бизнеса в области защиты критической информационной инфраструктуры

Обзор мировых практик



Взаимодействие государства и бизнеса в области защиты критической информационной инфраструктуры

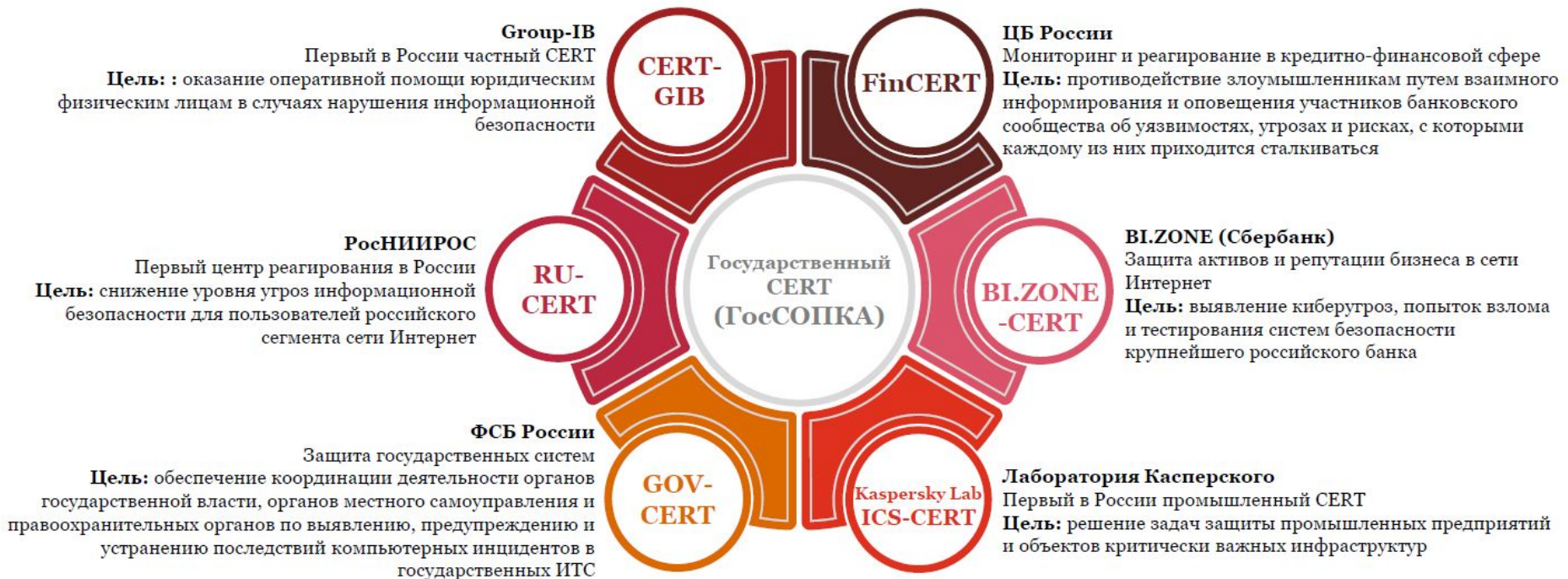
Инфраструктура государственного CERT



Ростелеком — не только один из крупнейших операторов связи, но и провайдер сервисов кибербезопасности (Managed Security Service Provider, MSSP).

Взаимодействие государства и бизнеса в области защиты критической информационной инфраструктуры

Обзор российских CERT



Взаимодействие государства и бизнеса в области защиты критической информационной инфраструктуры

Российский подход к национальной кибербезопасности (ФЗ-187)

Ведение реестра значимых объектов критической информационной инфраструктуры (КИИ), который включает в себя категоризацию объектов, детали цифрового взаимодействия объектов КИИ в телекоммуникационных сетях и др. информация

Разработка единых требований к кибербезопасности объектов КИИ, включая интеграцию в иерархическую структуру национального CERT (ГосСОПКА)

Проведение мероприятий по оценке степени защищенности КИИ от кибератак

Федеральный закон о безопасности критической информационной инфраструктуры Российской Федерации способствует развитию единого подхода, предназначенного для предотвращения, обнаружения и ликвидации последствий компьютерных атак на критичные объекты информационной инфраструктуры.

Взаимодействие государства и бизнеса в области защиты критической информационной инфраструктуры

Подход к национальной кибербезопасности в Европейском Союзе

Каждая из 28 стран ЕС должна создать один или несколько CERT, покрывающих все ключевые индустрии. Работа над уменьшением несоответствий в законодательстве стран ЕС

Главным центром для всех стран становится CERT-EU, который координирует национальные CERT стран-членов ЕС

Сотрудничество с коммерческими организациями-производителями средств защиты информации – это шаг к сокращению технологического разрыва с США для создания собственных технических решений защиты критической инфраструктуры

Директива по сетевой и информационной безопасности (NIS) дает возможность сосредоточить внимание на защите наиболее важных сервисов и активов государств - членов ЕС и позволит сократить разрыв в уровне зрелости ИБ стран ЕС.

Европейская комиссия подписала в июле 2016 года соглашение о создании государственно-частного партнерства для разработки единого подхода к обеспечению кибербезопасности.

ЕС инвестирует в данное объединение до € 450 млн в рамках своей программы исследований и инноваций Horizon 2020 на 2017-2020 гг. (4 года). Ожидается, что участники рынка кибербезопасности инвестируют в три раза больше: в общей сложности около €1800 млн.

Взаимодействие государства и бизнеса в области защиты критической информационной инфраструктуры

Сравнительный анализ практики обеспечения кибербезопасности КИИ

	США	Германия	Россия	Англия	ОАЭ	Китай
1. Существует ли законы/политики, требующие защиты критической инфраструктуры от угроз кибербезопасности?	✓	✓	✓	✓	✓	✓
1.1. Существует ли законы/политики, которые требуют (по крайней мере) ежегодного аудита кибербезопасности?	✓	~	✗	✗	-	✓
1.2. Существует ли законы/политики, которые требуют обязательное оповещение об инцидентах кибербезопасности?	✗	✓	~	✗	✗	✓
1.3. Существуют ли санкции в случае несоблюдения этих нормативных требований?	✓	✓	✓	✓	✓	✓
1.4. Эти нормативные требования применимы к частным компаниям?	~	✓	✓	✓	-	✓
2. Существует ли государственный центр реагирования на инциденты ИБ (CERT) или группа по реагированию на инциденты ИБ (CSIRT)?	✓	✓	~	✓	✓	✓
2.1. В каком году был создан государственный центр реагирования на чрезвычайные ситуации (CERT)?	2003	2012	2012	2014	2007	2002
2.2. Существуют ли некоммерческие организации, которые поддерживают инициативы или проекты, направленные на развитие, продвижение и поддержку кибербезопасности?	✓	✓	✗	✓	✓	✓
3. Существует ли государственный центр мониторинга информационной безопасности (SOC)?	✗	✓	✗	✗	✓	✓

~ - В процессе ✓ - Да ✗ - Нет

Центр реагирования на компьютерные инциденты в информационных системах органов государственной власти Российской Федерации GOV-CERT.RU



Центр реагирования на компьютерные инциденты в информационных системах органов государственной власти Российской Федерации
Международное название GOV-CERT.RU



[Главная](#)

[Инциденты](#)

[Контакты](#)

[Партнёрам](#)

[Сообщить об инциденте !\[\]\(05be7c7a8995decd503647c99211f7c2_img.jpg\)](#)

Информация о GOV-CERT.RU

Центр реагирования на компьютерные инциденты в информационно-телекоммуникационных сетях (ИТС) органов государственной власти Российской Федерации (GOV-CERT.RU) осуществляет координацию действий заинтересованных организаций и ведомств в области предотвращения, выявления и ликвидации последствий компьютерных инцидентов, возникающих в ИТС органов государственной власти Российской Федерации. GOV-CERT.RU решает следующие задачи:

- оказание консультативной и методической помощи при проведении мероприятий по ликвидации последствий компьютерных инцидентов в ИТС органов государственной власти РФ;
- анализ причин и условий возникновения инцидентов в ИТС органов государственной власти РФ;
- выработка рекомендаций по способам нейтрализации актуальных угроз безопасности информации;
- взаимодействие с российскими, иностранными и международными организациями, осуществляющими реагирование на компьютерные инциденты; накопление и анализ сведений о компьютерных инцидентах.

Контакты:

телефон - +7 (916) 901-07-42

почта - gov-cert@gov-cert.ru

Хотите сообщить о найденной уязвимости?

[Звоните или пишите нам!](#)

Центр реагирования на компьютерные инциденты в информационных системах органов государственной власти Российской Федерации

GOV-CERT.RU



Центр реагирования на компьютерные инциденты в информационных системах органов государственной власти Российской Федерации
Международное название GOV-CERT.RU




[Главная](#)

[Инциденты](#)

[Контакты](#)

[Партнёрам](#)

[Сообщить об инциденте](#) 

Зона ответственности GOV-CERT.RU

Деятельность GOV-CERT.RU направлена на повышение защищенности ИТС органов государственной власти Российской Федерации.

GOV-CERT.RU осуществляет реагирование на компьютерные инциденты, в которые вовлечены объекты, размещенные в сегменте RSNET (Russian State Network) сети Интернет, а также другие объекты информационной инфраструктуры РФ, принадлежащие органам государственной власти.

Виды угроз и инцидентов, на которые осуществляет реагирование GOV-CERT.RU

- атаки типа «отказ в обслуживании» в отношении ИТС органов государственной власти РФ;
- вовлечение объектов ИТС в бот-сети и распространение вредоносного ПО;
- попытки несанкционированного доступа к объектам ИТС органов государственной власти РФ.

В случае возникновения угроз, не входящих в данный перечень, решение о реагировании на них силами GOV-CERT.RU принимается в каждом случае индивидуально.

Контакты:

телефон - +7 (916) 901-07-42
почта - gov-cert@gov-cert.ru

Хотите сообщить о найденной уязвимости?

[Звоните или пишите нам!](#)

Центр реагирования на компьютерные инциденты в информационных системах органов государственной власти Российской Федерации GOV-CERT.RU



Центр реагирования на компьютерные инциденты в информационных системах органов государственной власти Российской Федерации
Международное название GOV-CERT.RU



[Главная](#)

[Инциденты](#)

[Контакты](#)

[Партнёрам](#)

[Сообщить об инциденте](#) 

Как с нами связаться?

Для связи с центром реагирования на инциденты в информационных системах органов государственной власти Российской Федерации можно использовать электронную почту, телефон или отправить сообщение через соответствующую форму на сайте.

- Телефон (с 9:00 до 18:00 в рабочие дни): +7 (916) 901-07-42
- Электронная почта: gov-cert@gov-cert.ru

Для защиты передаваемой информации и подтверждения подлинности отправителя при электронной переписке GOV-CERT.RU использует PGP (Pretty Good Privacy).

- [Получить открытый ключ PGP](#)
- Отпечаток ключа: 4D72 E5BD EA7F 046E 6C33 FB86 B6B8 3E23 25D8 A13B

Контакты:

телефон - +7 (916) 901-07-42
почта - gov-cert@gov-cert.ru

Хотите сообщить о найденной уязвимости?

[Звоните или пишите нам!](#)

Центр реагирования на компьютерные инциденты в информационных системах органов государственной власти Российской Федерации GOV-CERT.RU



Центр реагирования на компьютерные инциденты в информационных системах органов государственной власти Российской Федерации
Международное название GOV-CERT.RU



[Главная](#)

[Инциденты](#)

[Контакты](#)

[Партнёрам](#)

[Сообщить об инциденте](#)

Сообщить об инциденте

Тема сообщения

Название организации или ИТС

Должность, фамилия и имя лица, сообщившего об инциденте

Контактная информация (телефон, факс, адрес электронной почты)

Дата и время обнаружения инцидента

Описание выявленного инцидента (характер воздействия, описание объектов, вовлеченных в инцидент, источник воздействия, наличие лог-файлов, и другие сведения об инциденте)

Введите символы на картинке:



До проведения мероприятий по реагированию на компьютерные инциденты GOV-CERT.RU предпринимает меры по проверке достоверности поступающих сведений.

Контакты:

телефон - +7 (916) 901-07-42

почта - gov-cert@gov-cert.ru

Хотите сообщить о найденной уязвимости?

[Звоните или пишите нам!](#)

Центры реагирования на компьютерные инциденты в РФ

GOV-CERT.RU не единственный, кто занимается реагированием на инциденты.

До 2016 года в России таких организаций (исключая GOV-CERT) было всего три - CERT-GIB, WebPlus ISP и RU-CERT. В 2016 г. в дополнение к ним начали функционировать Kaspersky Lab ICS-CERT, а также FinCERT.

Основатель CERT-GIB - компания Group-IB. Этот CERT - сугубо частный центр реагирования, обслуживающий сторонние организации, а также претендующий на звание "прогосударственного", т.к. именно с ним Координационным центром национального домена сети Интернет было заключено соглашение о противодействии киберугрозам в доменах .RU и .РФ (наряду с подразделением Лиги безопасного Интернета - фондом "Дружественный Рунет").

Webplus ISP CERT занимается обслуживанием только собственных ресурсов, а вот RU-CERT, претендуя на звание национального CERTа, все-таки таковым не является. Хотя он является первым центром реагирования в России.

RU-CERT входит в международные объединения CERTов - FIRST и Trusted Introducer, являясь точкой контакта от России. RU-CERT - единственный, кто от России пока входит в FIRST, но не единственный, кто входит в Trusted Introducer - CERT-GIB и Webplus ISP тоже туда входят. Разница только в том, что RU-CERT имеет статус аккредитованного, а CERT-GIB и Webplus просто в списке CERT'ов. Но на работу это никак не влияет.

CERT-GIB - центр круглосуточного реагирования на инциденты информационной безопасности, созданный на базе компании Group-IB.

cert.group-ib.ru

НАВИГАЦИЯ

GROUP | IB

РУССКИЙ

ENGLISH



Центр реагирования CERT-GIB

CERT-GIB (Computer Emergency Response Team – Group-IB) – центр круглосуточного реагирования на инциденты информационной безопасности.

Мы оказываем помощь в реагировании на следующие типы инцидентов:

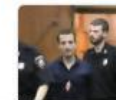
- DoS / DDoS атаки
- Распространение вредоносного программного обеспечения

- Появление мошеннических интернет-ресурсов
- Несанкционированный доступ и компрометация информационных систем
- Инциденты, связанные с бот-сетями
- Фишинг и незаконное использование бренда в сети Интернет
- Атаки на ДБО и электронные платежные системы

ТВИТЫ от @CERTGIB

 **CERT-GIB**
@CERTGIB

В США осудили на 12 лет хакера из России.
Russian hacker sentenced to 12 years' imprisonment.
xakep.ru/2016/07/07/stu...



В США осудили на 12 лет хак...
В США был вынесен приговор ...
xakep.ru

CERT-GIB - центр круглосуточного реагирования на инциденты информационной безопасности, созданный на базе компании Group-IB.



МЫ ГОТОВЫ ПОМОЧЬ ВАМ КРУГЛОСУТОЧНО, 7 ДНЕЙ В НЕДЕЛЮ, 365 ДНЕЙ В ГОДУ

CERT-GIB – это:



Квалифицированная помощь специалистов с многолетним опытом реагирования на киберпреступления



Оперативное блокирование опасных сайтов в доменах .RU, .РФ и еще более чем 1100 доменных зонах



Возможность принятия мер за пределами рунета посредством взаимодействия с Центрами реагирования CERT в других странах и международными ассоциациями по борьбе с киберпреступлениями



Круглосуточный мониторинг появления опасных сайтов и поддержка «горячей линии» для информирования о подозрительных ресурсах – [«Антифишинг»](#)

CERT-GIB - центр круглосуточного реагирования на инциденты информационной безопасности, созданный на базе компании Group-IB.



Компетентная организация [Координационного центра национального домена сети Интернет](#) и [Фонда развития Интернета](#).



Аккредитованный член международных сообществ [FIRST](#) и [Trusted Introducer](#), объединяющих команды реагирования на инциденты информационной безопасности



Партнер [IMPACT](#) – международного многопрофильного партнерства по противодействию киберугрозам



Центр реагирования, официально авторизованный Университетом Карнеги — Меллон ([Carnegie Mellon University](#)) и обладающий разрешением на использование торговой марки «CERT»

Предотвращение	Реагирование	Расследование	Bot-Trek	О Group-IB	Связаться с нами
Аудит безопасности	Центр реагирования CERT	Отдел расследований	Bot-Trek Intelligence	Компания	Круглосуточная линия +7 495 984-33-64
Антипиратство		Лаборатория криминалистики	Bot-Trek TDS	Медиа-центр	
Защита бренда		Кейсы	Bot-Trek Secure Bank	Команда	Электронная почта info@group-ib.ru
Защита от DDoS-атак			Bot-Trek Secure Portal	Партнеры	
				Клиенты	Адрес офиса
				Вакансии	Москва, улица Шарикоподшипниковская,
				Контакты	д.1, БЦ «Прогресс Плаза», 9 этаж



CERT-GIB - центр круглосуточного реагирования на инциденты информационной безопасности, созданный на базе компании Group-IB.



Официальный партнер [Europol](#), полицейской службы Евросоюза



Компания, рекомендованная Организацией по безопасности и сотрудничеству в Европе ([ОБСЕ](#))



Одна из 7 самых влиятельных компаний в области кибер-безопасности по версии [Business Insider](#)



Первый российский поставщик threat intelligence решений, вошедший в отчеты [Gartner](#)



Лицензии Федеральной Службы по Техническому и Экспортному Контролю (ФСТЭК России) на деятельность по технической защите конфиденциальной информации, серия КИ 0141 № 007032, регистрационный номер 2858 и на деятельность по разработке и производству средств защиты конфиденциальной информации, серия КИ 0141 регистрационный номер 007033



Лицензии Федеральной Службы Безопасности (ФСБ России) на работу со сведениями, составляющими государственную тайну, серия ГТ № 0064472, регистрационный номер 4490 и на осуществление разработки, производства, распространения шифровальных средств, информационных и телекомм. систем, серия ЛСЗ № 0012507, регистрационный номер 15000 Н

CERT-GIB - центр круглосуточного реагирования на инциденты информационной безопасности, созданный на базе компании Group-IB.

“В США существует не менее 62 команд по реагированию на инциденты информационной безопасности, в Дании — семь, а в России, самой большой стране мира, до образования CERT-GIB была только одна. Назрела необходимость в создании еще одной структуры, способной в кратчайшие сроки решать проблемы информационной безопасности, возникающие на территории РФ или затрагивающих российские организации”.

Илья Сачков, генеральный директор Group-IB.

CERT-GIB - центр круглосуточного реагирования на инциденты информационной безопасности, созданный на базе компании Group-IB.

Миссия CERT-GIB

координация обмена информацией об инцидентах информационной безопасности (далее – инциденты ИБ) между правоохранительными органами, юридическими и физическими лицами;

содействие в поддержании кибербезопасности в российском сегменте Интернета и за его пределами;

содействие в оперативном управлении киберрисками и устранение источников виртуальных угроз.

В рамках данной миссии, CERT-GIB предоставляет бесплатное круглосуточное информационное содействие по вопросам безопасности и реагирования на инциденты ИБ в Рунете. Ниже представлены примеры некоторых функций CERT-GIB:

предоставление начальной поддержки и рекомендаций по DDoS-инцидентам;

информирование затронутых сторон - физических и юридических лиц - о зафиксированных случаях фрода;

оказание помощи пострадавшей стороне в налаживании контактов с регистраторами, хостинг-провайдерами и правоохранительными органами РФ и бывшего СССР;

реагирование на предмет нейтрализации мошеннических сайтов, таких как фишинг, поддельные банковские сайты, скам-сайты, источники нарушения авторских прав и другие типы злонамеренных ресурсов.

При реализации своей миссии CERT-GIB не берет на себя обязательства по управлению и поддержке ИТ-инфраструктуры обратившегося лица.

CERT-GIB - центр круглосуточного реагирования на инциденты информационной безопасности, созданный на базе компании Group-IB.

Структура CERT-GIB

CERT-GIB является на текущий момент первым и единственным негосударственным CERT на территории Российской Федерации, который оказывает помощь любым обратившимся физическим и юридическим лицам.

CERT-GIB представляет собой подразделение оперативного реагирования, созданное на базе Group-IB.

Для обеспечения непрерывного оперативного цикла работы CERTа, сбор информации и реагирование на инциденты осуществляется в режиме 24/7/365 – из трех центров географических дислокаций представительств CERT-GIB: Москвы, Нью-Йорка и Сингапура.

Взаимосвязь между CERT-GIB и другими организациями CERT

Во всем мире существует около трехсот организаций, использующих аббревиатуру «CERT» (либо схожую) в своем названии – большинство из них являются командами быстрого реагирования на инциденты информационной безопасности.

Хотя прямой зависимости между CERT-GIB и другими CERT/CSIRT не существует, CERT-GIB постоянно поддерживает связь с большинством этих организаций и, при необходимости, можем напрямую координировать с ними действия, связанные с инцидентами ИБ.

CERT-GIB - центр круглосуточного реагирования на инциденты информационной безопасности, созданный на базе компании Group-IB.

Взаимодействие с представителями сектора ИБ, правоохранительными органами и СМИ

Взаимодействие с производителями программных продуктов, аппаратных средств и средств защиты информации производится с целью информирования об обнаруженных уязвимостях в их продуктах, а также для разработки мер по защите ИТ-активов Клиентов от актуальных угроз ИБ.

Взаимодействие с правоохранительными органами осуществляется на основе официальных запросов в соответствии с текущим законодательством РФ. CERT-GIB оказывает максимальное содействие в расследовании правонарушений, в которых были задействованы ИТ-активы, входящие в зону ответственности CERT-GIB.

Взаимодействие со средствами массовой информации производится через PR-службу CERT-GIB. CERT-GIB не дает комментарии по инцидентам, возникшим в зоне ответственности, без согласия Клиента.

Кто может обратиться в CERT-GIB?

Обратиться в CERT-GIB может **любое** физическое или юридическое лицо, пострадавшее от инцидента ИБ, либо желающее сообщить об известном инциденте.

На какие инциденты ИБ можно пожаловаться?

Инцидент информационной безопасности - одно или серия нежелательных событий, которые имеют большой шанс поставить под угрозу защиту информации.

Примеры подобных инцидентов:

Фишинг и незаконное использование бренда в сети Интернет;

Рассылка СПАМа;

Несанкционированное распространение защищённых авторским правом материалов;

Мошеннические ресурсы и мошеннические схемы в сети Интернет;

DoS/DDoS атаки;

Распространение вредоносного ПО;

Попытки компрометации информационных систем.

Кому будет доступна информация об инциденте?

Вся информация, получаемая командой CERT-GIB, обрабатывается как конфиденциальная, что исключает возможность доступа к ней третьих лиц, если не было оговорено обратного.

Какую информацию необходимо включать в заявку?

Заявление должно содержать краткое описание и дату произошедшего или обнаруженного инцидента. Также заявление может содержать дополнительную информацию, которую заявитель считает важной.

Для чего сообщать об инциденте ИБ?

Вся получаемая CERT-GIB информация обрабатывается и, в зависимости от типа инцидента ИБ, предпринимаются необходимые действия для нейтрализации последствий. В том числе происходит оповещение пострадавших и заинтересованных сторон, выявление и устранение проблем, а также поиск причин возникшего инцидента для предотвращения подобных ситуаций в будущем. Таким образом, сообщая об инцидентах специалистам CERT-GIB, Вы участвуете в повышении уровня защищённости сети Интернет.

Как можно обратиться в CERT-GIB?

Круглосуточно сообщить об инциденте возможно любым из представленных способов:
Телефон: +7 (495) 988-00-40; Email: response@cert-gib.ru; Форма обратной связи: <http://cert-gib.ru/report.php>

Центр реагирования на компьютерные инциденты Webplus ISP CERT

Яндекс security.wplus.net/index.html

Вэб Плас Подключение без приключений ■ Санкт-Петербург ■ English

ADSL канал Клонирование телефонов Умные сети Интернет карты Телефонные карты Веб-сайты хостинг

поиск о компании новости услуги и цены тех. поддержка оплата контакты

Контактная информация

Круглосуточная служба сервис-центра может оказать Вам первоочередную помощь при возникновении у Вас проблем с безопасностью в Интернете. Связаться с ней можно по телефону 3269020 или по электронной почте по адресу support@wplus.net

Для решения более сложных вопросов обращайтесь к ответственному за информационную безопасность по адресу: security@wplus.net.

- Управление почтой
- Ваши домашние странички
- Настройки
- ▶ **Безопасность**
 - Информация
 - Тесты на безопасность
 - Программы
 - Пользователям
 - Контакты
 - Ссылки
- Полезные ссылки
- Задать вопрос

Центр реагирования на компьютерные инциденты Webplus ISP CERT

Обязательно установите на ВСЕ компьютеры, с которых Вы пользуетесь услугами "Вэб Плас", антивирусную программу для защиты от троянских коней и вирусов в режиме резидентного монитора (тогда она будет проверять все запускаемые программы и открываемые документы автоматически). Мы рекомендуем Вам использовать AVP или DrWeb. Обновляйте антивирусные базы данных не реже, чем каждые 1-3 дней. Большинство антивирусов позволяют делать это бесплатно и через Интернет. Если антивирусная база не обновлялась более 3 месяцев, эффективность антивируса сильно снижается.

Для защиты от неизвестных вирусов и троянских коней также можно установить программу-ревизор, осуществляющую контроль целостности файлов. Необъяснимые изменения файлов или появление новых файлов, обнаруженных ею, являются признаками появления нового вируса или троянского коня.

Помните, что смена пароля не спасает, если идентификационные параметры украдены троянским конем. Троянский конь будет продолжать красть их до тех пор, пока он не будет удален с компьютера. Поэтому установите антивирус на компьютер, если Вы этого не сделали. Регулярно (не реже 1 раз в неделю) смотрите статистику использования Вами Интернет и Ваш денежный баланс. Если Вы заметили входы в Интернет, которых вы не делали - срочно смените пароль.

Регулярно (не реже 1 раз в месяц) меняйте Ваш пароль. Если Вы подозреваете, что кто-то мог его узнать - срочно смените пароль.

Ограничьте доступ к Вашему компьютеру с помощью программ управления доступом и установки требования ввода пароля BIOSом при включении компьютера.

Делайте резервные копии системных файлов и важных данных и храните их в безопасном месте (не на жестком диске Вашего компьютера). В случае сбоя жесткого диска или вирусной атаки это позволит Вам быстро продолжить работу.

Центр реагирования на компьютерные инциденты Webplus ISP CERT

Помните, что программы, которыми Вы пользуетесь при работе в Интернет, могут содержать ошибки безопасности (уязвимости). Эти ошибки могут позволить злоумышленнику заблокировать Ваш компьютер или получить несанкционированный доступ к нему через Интернет. Производители операционных систем и прикладных программ регулярно публикуют информацию об обнаруженных уязвимостях (например, Microsoft имеет web-сайт - www.microsoft.com/security/) и исправленные версии программ. Проверьте, что Вы установили ВСЕ исправления для используемых Вами операционной системы и программ, и если нет - сделайте это как можно скорее. Следите за публикациями о новых обнаруженных ошибках в программах и оперативно устанавливайте исправления для них. Рекомендуем для этого подписаться на список рассылки на сайте www.sans.org.

Для повышения безопасности следует установить на компьютере персональный пакетный фильтр - программу, которая поможет защитить Ваш компьютер от несанкционированного доступа злоумышленников к нему через Интернет, даже если на компьютере установлен троянский конь или программы содержат уязвимости, путем блокирования некоторых принимаемых и передаваемых пакетов. Для диалап-пользователей делать это не обязательно, так как по умолчанию Вы уже защищены пакетным фильтром, установленным на нашем сервере доступа (у Вас уже установлен стандартный уровень защиты). Он позволяет защититься от типовых атак из Интернет. Если Вы хотите, то можете сами установить себе индивидуальный уровень защиты с помощью фильтрации пакетов на сервере доступа "Вэб Плас" .

Не думайте, что вирусы и троянские кони могут находиться только в программах, загруженных из Интернета - как показывает печальный опыт покупателей пиратских CD, на них все чаще появляются программы, также зараженные вирусами или троянскими конями. Если уж Вы купили CD, проверьте его хорошей антивирусной программой с последней антивирусной базой данных.

Используйте PGP (www.pgpi.org) для шифрования своих важных писем и добавления к ним своей электронной подписи при переписке со своими корреспондентами в Интернете (при установке она автоматически вставляется в Eudora, Outlook и TheBat и легко может быть вызвана из них).

Центр реагирования на компьютерные инциденты Webplus ISP CERT

Рекомендации по обеспечению безопасности для пользователей услуг авторизуемого доступа.

Не запускайте у себя на компьютере программ из ненадежных источников и не открывайте приложения к письмам, даже если письмо пришло от Вашего хорошего знакомого - в них могут быть спрятаны вирусы или троянские кони. Сначала сохраните это приложение в файл и проверьте его антивирусной программой. Помните, что злоумышленники могут прибегнуть к разнообразным приемам, чтобы обманом получить у Вас информацию об идентификационных параметрах или заставить Вас запустить программу, которая украдет у Вас их (такие программы называются троянскими конями). Будьте настороже и ознакомьтесь с информацией о типовых приемах обмана.

Не надо верить всем сообщениям о новых страшных вирусах, появившихся в Интернет, особенно если в сообщении сказано, что надо распространить эту информацию всем Вашим знакомым. Это сообщение может оказаться просто компьютерной шуткой.

Если Вы получили письмо от незнакомого человека или организации, то знайте, что скорее всего это спам - назойливые рекламные письма и письмо попало в Ваш ящик не по ошибке, а специально. Чтобы не получать письма от этого адресата впредь, нужно написать жалобу администратору сети, откуда прислано это письмо.

ЦЕНТР РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ Российской Федерации RU-CERT

RU-CERT, создан НИИ развития общественных сетей

www.cert.ru/ru/about.shtml

Русский | English



Центр реагирования
на компьютерные инциденты
Российской Федерации

RU-CERT

Инциденты

Контакты

Сообщить об инциденте

RU-CERT

RU-CERT – российский центр реагирования на компьютерные инциденты. Основная задача центра – снижение уровня угроз информационной безопасности для пользователей российского сегмента сети Интернет. В этих целях RU-CERT оказывает содействие российским и зарубежным юридическим и физическим лицам при выявлении, предупреждении и пресечении противоправной деятельности, имеющей отношение к расположенным на территории Российской Федерации сетевым ресурсам.

RU-CERT осуществляет сбор, хранение и обработку статистических данных, связанных с распространением вредоносных программ и сетевых атак на территории РФ.

Для реализации поставленных задач RU-CERT взаимодействует с ведущими российскими IT-компаниями, субъектами оперативно-розыскной деятельности, органами государственной власти и управления РФ, зарубежными центрами реагирования на компьютерные инциденты и другими организациями, осуществляющими свою деятельность в области компьютерной и информационной безопасности.

RU-CERT входит в состав международных объединений CSIRT / CERT центров [FIRST](#) и [Trusted Introducer](#), и в рамках данных объединений официально выполняет функции контактной стороны в Российской Федерации.

Действуя в рамках нормативной правовой базы РФ, RU-CERT не уполномочен заниматься решением вопросов, находящихся в ведении правоохранительных органов. В этих случаях необходимо обращаться в региональные подразделения ФСБ или МВД РФ.

ЦЕНТР РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ Российской Федерации RU-CERT

Инциденты

В качестве компьютерных инцидентов в RU-CERT рассматриваются факты и признаки нарушений российского и международного законодательства при работе в сети Интернет, а также принятых большинством пользователей сети норм и правил ее использования.

В первую очередь при реагировании на компьютерные инциденты RU-CERTом принимаются во внимание оценка степени надежности и доверия источника информации и наличие технических возможностей проведения проверки указанного факта. RU-CERT не уведомляет пользователей о результатах и характере предпринимаемых действий.

RU-CERT не обладает полномочиями по закрытию ресурсов, фильтрации адресов, прекращению делегирования доменов, удалению контента с того или иного ресурса, поиску лиц, причастных к тем или иным действиям и т.п.

RU-CERT обеспечивает сервис по реагированию на инциденты без каких-либо гарантий и обязательств.

RU-CERT не фиксирует и не регистрирует факты рассылки СПАМ сообщений.

RU-CERT гарантирует конфиденциальность всей полученной информации и ее нераспространение без согласия обратившейся стороны, за исключением случаев, оговоренных законодательством РФ.

Контакты

Полное наименование организации

Автономная некоммерческая организация (АНО) «Центр реагирования на компьютерные инциденты» (ЦРКИ). Russian Computer Emergency Response Team (RU-CERT).

Почтовый адрес: 123060, г. Москва, ул. Расплетина, д. 4, корп. 1.

Телефон / факс: Телефон: +7 499 1969010, +7 499 1967221. Факс: +7 499 1974892.

Часы работы: Ежедневно с 10:00 до 18:00 кроме выходных дней и национальных праздников.

E-mail: info@cert.ru



Центр реагирования
на компьютерные инциденты
Российской Федерации

RU-CERT

Инциденты

Контакты

Сообщить об инциденте

Сообщить об инциденте

По электронной почте

Через web-форму ▾

Сообщить об инциденте можно путем отправки сообщения на [✉ адрес электронной почты](#). Электронная почта является предпочтительным способом связи с сотрудниками RU-CERT.

Для защиты передаваемой информации и подтверждения подлинности при обмене почтовыми сообщениями Вы можете использовать программное обеспечение стандарта [PGP / OpenPGP](#) и соответствующий [↓ публичный ключ RU-CERT](#).

Центр реагирования на компьютерные инциденты на промышленных и критически важных объектах – Kaspersky Lab ICS-CERT

В ходе конференции «Кибербезопасность АСУ ТП 2016: время действовать вместе», которая проходила в Иннополисе с 10 по 12 октября 2016 года, «Лаборатория Касперского» объявила об открытии первого в России центра реагирования на компьютерные инциденты на промышленных и критически важных объектах – Kaspersky Lab ICS-CERT.

Основная цель ICS-CERT «Лаборатории Касперского» – координировать действия производителей систем автоматизации, владельцев и операторов промышленных объектов, а также исследователей в области информационной безопасности. CERT будет собирать информацию о найденных уязвимостях, имевших место инцидентах и актуальных угрозах и на основе этих данных предоставлять рекомендации по защите промышленных и критически важных инфраструктурных объектов. Все данные, за исключением конфиденциальных, будут доступны публично в обезличенном виде. Что касается сведений об уязвимостях в промышленном ПО и оборудовании, то они будут публиковаться при взаимодействии с производителями согласно политике ответственного разглашения.

Помимо этого, ICS-CERT планирует проводить консультации по требованиям государственных и отраслевых регуляторов в области обеспечения информационной безопасности промышленных объектов. Также специалисты центра смогут оценить уровень защищенности промышленных систем автоматизации и провести расследование инцидентов информационной безопасности.

Данные и услуги ICS-CERT будут доступны бесплатно заинтересованным организациям по всему миру. Ожидается, что основными клиентами центра станут производители компонентов АСУ ТП, национальные CERT и промышленные предприятия, работающие в самых разных отраслях: в энергетике, машиностроении, нефтегазовом секторе, металлургии, производстве строительных материалов, транспорте и пр. Также ICS-CERT «Лаборатории Касперского» готов сотрудничать со сторонними исследователями информационной безопасности, государственными органами и международными правоохранительными организациями.

Центр реагирования на компьютерные инциденты на промышленных и критически важных объектах – Kaspersky Lab ICS-CERT

KASPERSKY LAB ICS CERT

Kaspersky Lab Industrial Control Systems Cyber Emergency Response Team — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.



ОБЩАЯ ОЦЕНКА БЕЗОПАСНОСТИ



ТЕСТ НА ПРОНИКНОВЕНИЕ



УДАЛЁННОЕ ОБНАРУЖЕНИЕ



КООРДИНАЦИЯ И УСТРАНЕНИЕ



ИНФОРМАЦИЯ ОБ УГРОЗАХ

ОПОВЕЩЕНИЯ

Целевая фишинг-атака на промышленные компании

16 декабря 2016

[ЕЩЕ ОПОВЕЩЕНИЯ](#)

НОВОСТИ

В Далласе хакеры посреди ночи включили все тревожные сирены

11 апреля 2017

Пример от Talos, команды безопасности Cisco по исследованию промышленной беспроводной точки доступа Moxa

10 апреля 2017

Уязвимость в популярной библиотеке приводит многие промышленные устройства в незащищенное состояние

10 апреля 2017

ОТЧЕТЫ

Ландшафт угроз для систем промышленной автоматизации. Второе полугодие 2016

28 марта 2017

Глобальная статистика уязвимостей

09 декабря 2016

Управление безопасностью критической инфраструктуры в странах по всему миру

02 декабря 2016

[ЕЩЕ ОТЧЕТЫ](#)

УЯЗВИМОСТИ

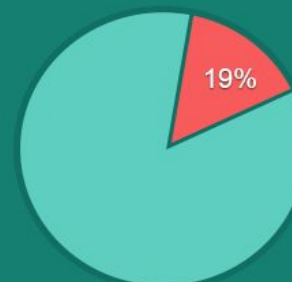
Уязвимость протокола Schneider Electric Modicon Modbus позволяет перехватывать и изменять команды к PLC

11 апреля 2017

INDUSTRIAL CYBERTHREATS REAL-TIME MAP



ПРОЦЕНТ АТАКОВАННЫХ ПРОМЫШЛЕННЫХ КОМПЬЮТЕРОВ, ФЕВРАЛЬ 2017

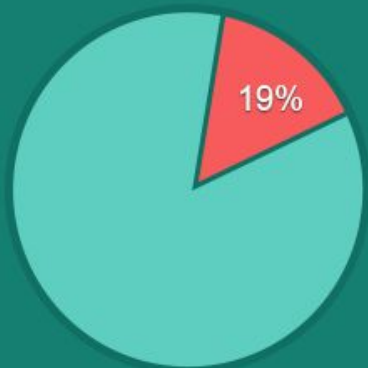


ТОП 15 СТРАН ПО ПРОЦЕНТУ АТАКОВАННЫХ ПРОМЫШЛЕННЫХ КОМПЬЮТЕРОВ, ФЕВРАЛЬ 2017

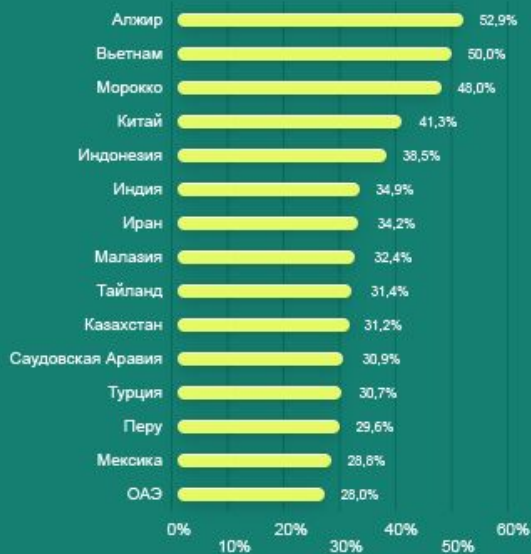


Центр реагирования на компьютерные инциденты на промышленных и критически важных объектах – Kaspersky Lab ICS-CERT

ПРОЦЕНТ АТАКОВАННЫХ ПРОМЫШЛЕННЫХ КОМПЬЮТЕРОВ, ФЕВРАЛЬ 2017



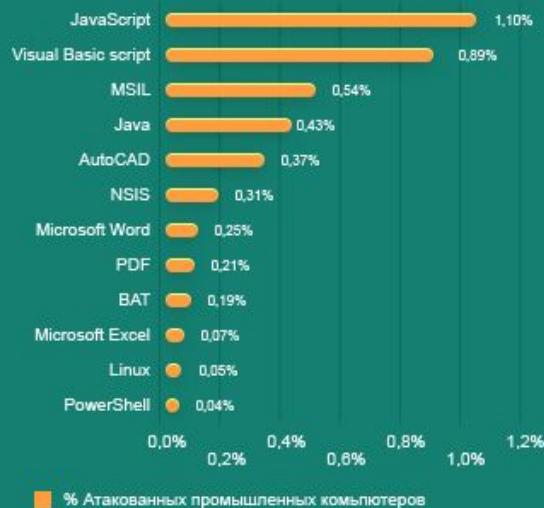
ТОП 15 СТРАН ПО ПРОЦЕНТУ АТАКОВАННЫХ ПРОМЫШЛЕННЫХ КОМПЬЮТЕРОВ, ФЕВРАЛЬ 2017



ИСТОЧНИКИ УГРОЗ, ФЕВРАЛЬ 2017



ПЛАТФОРМЫ ВРЕДНОСНОГО ПО, ФЕВРАЛЬ 2017



Центр реагирования на компьютерные инциденты на промышленных и критически важных объектах – Kaspersky Lab ICS-CERT

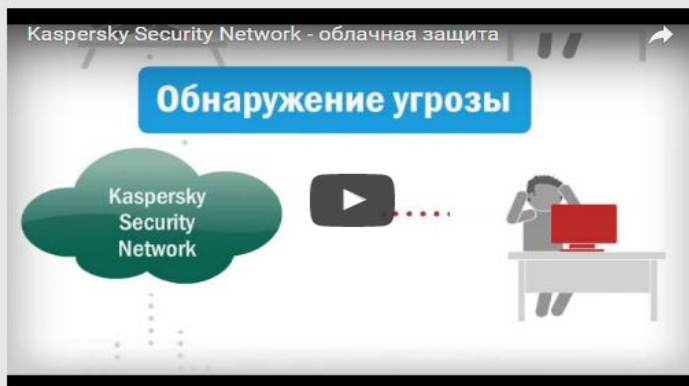
Информация об угрозах

ksn.kaspersky.com Kaspersky Security Network | Kaspersky Lab RU

KASPERSKY SECURITY NETWORK

Ни для кого не секрет, что компьютерные угрозы появляются каждый день тысячами. Чтобы их заблокировать, классическим антивирусным программам необходимо не менее 4,5 часов, пока специалисты не обнаружат угрозу и не внесут ее в базу сигнатур. Не спасают даже продвинутые эвристические методы детектирования. Их уровень правильного срабатывания, как правило, не выше 70%. Получается, что множество вредоносных программ, фишинговых сайтов и прочих угроз может беспрепятственно делать свое зловерное дело в течение нескольких часов.

Для противостояния современным угрозам производители антивирусов уделяют все больше внимания альтернативным методам их выявления и блокирования. Одним из таких методов, разрабатываемых в Лаборатории Касперского, является антивирусное облако – Kaspersky Security Network (KSN). Подробнее об этой технологии вы можете прочитать в статье нашего эксперта на Securelist.com.



С согласия пользователя антивирусного приложения в KSN отправляются данные о попытках заражения компьютера и о подозрительной активности программ. Полученные данные распределенно обрабатываются экспертной системой, и информация о только что появившихся угрозах и источниках их распространения становится доступной всем пользователям продукта в течение 40 секунд.

Антивирус, работа которого основывается на принципе защиты из облака, позволяет пользователям:

- в кратчайшее время быть защищенными от самых последних угроз;
- сократить трафик, расходуемый на обновления антивируса;
- лишней раз не отвлекаться на ложные срабатывания антивируса.

Содержание

Проблемы информационной безопасности АСУ ТП	2
Особенности современных технологических сетей.....	3
Организация сопряжения сегментов сети	3
Доступ к внешним системам и сетям	3
Изменение ландшафта угроз	4
Уязвимости в программном обеспечении АСУ ТП.....	5
Уязвимости, обнаруженные «Лабораторией Касперского»	6
Уровень опасности обнаруженных уязвимостей	7
Проблемы закрытия уязвимостей	8
Статистика угроз	9
Процент атакованных компьютеров	9
Источники заражения промышленных систем	11
География атак на промышленные системы	14
Вредоносное ПО на системах промышленной автоматизации	15
Ботнет-активность в промышленных сетях	16
Целевые атаки на промышленные компании	18
Целевая фишинговая атака на промышленные компании	19
APT-атаки.....	21
Заключение.....	22

Примечание автора: АРТ это сокращение от Advanced Persistent Threat, то есть сложная постоянная угроза. Термин стал популярен после разоблачительного материала в «Нью-Йорк таймс», где рассказывалось об атаке на эту газету, устроенной китайской военной структурой, теперь известной как АРТ 1. По своей сути это хакерские нападения с использованием автоматизированных средств проникновения, за счёт чего увеличивается как вероятность проникновения, так и его скрытность.

Центр реагирования на компьютерные инциденты на промышленных и критически важных объектах – Kaspersky Lab ICS-CERT

https://ics-cert.kaspersky.ru/services/



Услуги

Контакты

[Главная](#) / [Услуги](#)

УСЛУГИ

АНАЛИЗ НА СООТВЕТСТВИЕ

«Лаборатория Касперского» предлагает сервис по анализу соответствия конфигурации сетевой инфраструктуры АСУ ТП, средств безопасности, организации доступа к информационным системам технологической сети, уровня осведомленности сотрудников предприятия и внешних подрядчиков о политиках информационной безопасности, а также их практических навыков в области защиты от кибер угроз требованиям государственных и отраслевых регуляторов.



ЗАПРОСИТЬ

ДАННЫЕ ПО УЯЗВИМОСТЯМ

Опираясь на результаты наших собственных исследований и исследований наших партнеров и агрегируя данные из различных публичных источников, мы получаем информацию о наиболее серьезных уязвимостях в продуктах, использующихся в АСУ ТП. В рамках данного сервиса мы предоставляем заказчику информацию об уязвимостях в программных и программно-аппаратных компонентах его систем промышленной автоматизации.



ПОДПИСАТЬСЯ

ИНФОРМАЦИЯ ОБ УГРОЗАХ

Имея обширную сеть источников информации о вредоносном ПО, насчитывающую более 60 000 000 компонентов, мы обнаруживаем и отслеживаем появление новых угроз по всему земному шару в режиме реального времени. В рамках данного сервиса мы предоставляем аналитические отчеты об угрозах, актуальных для вашей индустрии и вашего региона, и своевременно оповещаем о тех из них, которые могут представлять серьезную опасность для вашего предприятия.



ПОДПИСАТЬСЯ

Центр реагирования на компьютерные инциденты на промышленных и критически важных объектах – Kaspersky Lab ICS-CERT



УДАЛЁННОЕ ВЫЯВЛЕНИЕ

Как показывают наши собственные исследования и исследования ведущих мировых компаний и организаций, занимающихся обеспечением информационной безопасности, для крупных предприятий наибольшую опасность представляет человеческий фактор и атаки на цепочку поставки. Даже надежная система безопасности не защищает от всех атак со стороны сотрудника, поставщика или подрядчика. В рамках данного сервиса наши эксперты определяют проблемы информационной безопасности на вашем предприятии, связанные с этими факторами риска. Мы выявим угрозы с этой стороны, проверим наличие в публичном доступе конфиденциальных сведений о ваших системах автоматизации, а также информации, которая может быть использована для подготовки и проведения атак.



ЗАПРОСИТЬ



ОБЩАЯ ОЦЕНКА БЕЗОПАСНОСТИ

Мы предлагаем сервис по оценке состояния информационной безопасности сетей АСУ ТП промышленных организаций. Целью исследования является определение уязвимых мест сетевой инфраструктуры АСУ ТП, которые могут стать источником киберинцидентов, привести к нарушению целостности и работоспособности компонентов системы и нарушению непрерывности технологического процесса, что может привести к негативным последствиям для предприятия в целом. Исходными данными для анализа служат документированные сведения о технологической сети предприятия и информационных системах АСУ ТП. В ряде случаев дополнительная информация о системах предприятия может быть собрана инструментальным способом с использованием специальных средств и утилит.



ЗАПРОСИТЬ



ТЕСТ НА ПРОНИКНОВЕНИЕ

Мы предлагаем сервис тестирования сетевой инфраструктуры на проникновение в среду АСУ ТП. Подобное тестирование является эффективным средством проверки защищенности сетевой инфраструктуры предприятия от кибератак. В процессе тестирования наши специалисты определяют способы проникновения из внешних сетей во внутренний периметр технологической сети предприятия (векторы атак). Дополнительно Пентест может использоваться для проверки эффективности изменений в информационных системах предприятия, выполненных по результатам *Общей оценки состояния информационной безопасности предприятия*.



ЗАПРОСИТЬ

Центр реагирования на компьютерные инциденты на промышленных и критически важных объектах – Kaspersky Lab ICS-CERT

Информационные сервисы



АНАЛИЗ ЗЛОВРЕДОВ

В случае обнаружения вредоносного ПО в технологической сети предприятия мы можем провести анализ обнаруженного экземпляра в нашей лаборатории и предоставить вам описание основных свойств и функциональных возможностей данного вредоносного ПО для дальнейшей оценки вероятных причин и последствий инцидента.



ЗАПРОСИТЬ



АНАЛИЗ АРТЕФАКТОВ

Организациям, способным самостоятельно обнаружить и нейтрализовать кибер инциденты в технологической сети, мы готовы помочь с анализом информации, собранной со скомпрометированных во время атаки объектов (рабочих станций, сетевых устройств, программируемых устройств, USB-устройств и пр.). Анализ могут подвергаться образы диска скомпрометированного устройства, образ памяти, запись сетевой активности. По итогам анализа мы предоставим вам описание найденных следов компрометации устройства, обнаруженной вредоносной активности и вредоносного программного обеспечения.



ЗАПРОСИТЬ



КООРДИНАЦИЯ И УСТРАНЕНИЕ

Отслеживая возникновение и распространение угроз информационной безопасности промышленных предприятий при помощи наших собственных средств обнаружения и анализа угроз (см. «Информация о релевантных угрозах»), мы можем обнаружить атаку, направленную против вашего предприятия. Мы также готовы принять участие в расследовании инцидента, связанного с атакой на информационные системы предприятия, обнаруженной вами самостоятельно. Мы оказываем помощь в исследовании причины инцидента, деталей его возникновения и развития, масштабов воздействия атаки на информационные и технологические системы предприятия и предлагаем меры по предотвращению подобных инцидентов в будущем.



ЗАПРОСИТЬ

Центр реагирования на компьютерные инциденты на промышленных и критически важных объектах – Kaspersky Lab ICS-CERT

[Главная](#) / [Контакты](#)

КОНТАКТЫ

Для получения дополнительной информации по условиям предоставления сервисов кратко опишите ваши вопросы и пожелания и отправьте их по электронной почте на адрес ics-cert@kaspersky.com. Наши дежурные сотрудники свяжутся с вами в рабочее время с 9 до 18 часов по московскому времени.

ЦЕНТРАЛЬНЫЙ ОФИС «ЛАБОРАТОРИИ КАСПЕРСКОГО» ▾



Россия, Москва, 125212
Ленинградское шоссе, д.39А,
стр.3
БЦ «Олимпия Парк»



Электронная почта:
ics-cert@kaspersky.com

СООБЩИТЬ О ПРОИСШЕСТВИИ

KL ICS CERT стремится оперативно реагировать на заявки наших пользователей. Для точного определения причин и подготовки средств обнаружения / устранения, мы должны получить подробное описание возникшего инцидента. Пожалуйста, укажите в вашем сообщении как можно больше деталей о случившемся инциденте.

Описание:

Контактные данные (email, телефон):



Я не робот



reCAPTCHA

[Конфиденциальность](#) - [Условия использования](#)



СОЗДАТЬ ОТЧЕТ О
ПРОИСШЕСТВИИ

Центр реагирования на компьютерные инциденты на промышленных и критически важных объектах – Kaspersky Lab ICS-CERT

«Белым хакерам» удалось взломать смоделированную энергосистему, построенную на основе архитектуры microgrid*, и нарушить ее работу менее чем за сутки. Именно так закончился турнир по промышленной кибербезопасности, организованный «Лабораторией Касперского». Финал конкурса прошел в Иннополисе, в рамках четвертой всероссийской конференции по защите АСУ ТП «Время действовать вместе». За главный приз боролись четыре команды из Долгопрудного (Московская область), Екатеринбурга, Новосибирска и Саратова, победившие в предварительных отборочных этапах.

Всего для участия в CTF-турнире** зарегистрировалось 154 команды, преимущественно из России. Однако попытать свои силы во взломе энергосистемы на основе архитектуры microgrid также стремились участники из Белоруссии, Украины, Казахстана, Турции, Швеции, Румынии, Индии и Китая.

В рамках финала соревнующиеся команды в режиме реального времени атаковали и проверяли на прочность как отдельные компоненты энергосистемы, так и архитектуру в целом. Победившая команда Filthy Thg33 из Екатеринбурга смогла первой добиться успеха, то есть нарушила работу энергосистемы, устроила короткое замыкание, смоделировала локальное повреждение оборудования и лишила, таким образом, потребителей источника энергии (в рамках конкурса был смоделирован маленький город и завод).

«Условия наших CTF-турниров всегда максимально приближены к настоящим, потому что наша цель, прежде всего, состоит в том, чтобы понять потенциальные уязвимости и недочеты в критически важных инфраструктурах и промышленных системах, за счет которых живет сегодня весь мир. Так что каждая победа на CTF заставляет исследователей и разработчиков в очередной раз задуматься о том, как можно улучшить киберзащиту подобных объектов», – пояснил Владимир Дашенко, старший исследователь угроз в критической инфраструктуре «Лаборатории Касперского».

*Примечание автора: Существуют три типа энергетических микросетей: "Сеть первого типа снабжает энергией одно здание, обеспечивая его независимость от централизованной сети переменного тока.

Чаще всего встречается второй тип – кампусные сети, обеспечивающие энергией комплекс зданий на определенной территории. На этой территории создается внутренняя сеть распределения и внутренний источник энергии. Кампусная сеть, как и сеть первого типа, может работать независимо от централизованной энергосети".

Сеть третьего типа работает по методу Интернета, используя топологию сети распределения. "По мере увеличения надежности и устойчивости сетей, интеграции распределенных генерирующих мощностей и систем хранения энергии, сеть распределения начинает превращаться в совокупность взаимно подключенных микросетей, такие сети могут действовать совершенно независимо, а в экстренных случаях подключаться к внешним сетям". В последнем случае они будут связываться с сетями smart grid, повышая роль и значение сетевых соединений еще больше.

**CTF (Capture the flag) – это командная игра, главной целью которой является захват «флага» у соперника.

Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT)

Рост кибератак на кредитно-финансовые организации очевиден. Для эффективной борьбы с ними Банк России создал Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT), который осуществляет сбор и анализ информации от финансовых учреждений о кибератаках, а также предупреждает о возможных угрозах ИБ и взаимодействует с правоохранительными органами.



Дмитрий Фролов

Начальник Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России

Основной стратегической целью деятельности FinCERT – Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере – является повышение организациями, поднадзорными Банку России, эффективности мер по борьбе с противоправными действиями, осуществляемых при предоставлении финансовых услуг и услуг по переводу денежных средств с использованием информационных и телекоммуникационных технологий. Центр также проводит работу по противодействию компьютерным атакам на информационные ресурсы организаций, поднадзорных Банку России.

В качестве основных целей создания автоматизированной системы рассматриваются обеспечение двустороннего обмена данными как с Центром, так и с другими участниками информационного обмена и централизованное хранение данных о выявленных угрозах нарушения информационной безопасности.

Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT)

Главной задачей в рамках обозначенной цели является организация непрерывного взаимного информирования об угрозах нарушения информационной безопасности организаций, поднадзорных Банку России, и минимизация наносимого при реализации угроз материального ущерба. Для этого Центр собирает технические данные об угрозах нарушения информационной безопасности из следующих источников:

- организации, поднадзорные Банку России;
- государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА);
- органы исполнительной власти;
- правоохранительные органы;
- иные организации, например, антивирусные компании, вендоры программного обеспечения, регистраторы доменных имен;
- средства массовой информации/Интернет;
- физические лица.

Повышение уровня доверия к деятельности Центра должно произойти естественным путем после создания удобного и надежного интерфейса для информационного взаимодействия и обеспечения оперативного реагирования на выявленные угрозы нарушения информационной безопасности.

Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT)

Среди наиболее актуальных угроз нарушения информационной безопасности организаций, поднадзорных Банку России, стоит отметить следующие:

- целевые атаки на платежные автоматизированные системы кредитных организаций;
- неправомерный доступ к конфиденциальной компьютерной информации;
- использование вредоносного программного обеспечения;
- распределенный отказ в обслуживании (DDoS-атаки);
- мошенничество с использованием электронной почты;
- мошенничество с использованием средств сотовой связи;
- мошенничество с использованием номеров в коде "8-800".

Необходимо организовать обмен следующими данными:

- IP-адреса, с которых осуществляются DDoS-атаки;
- IP-адреса, с которых осуществляется рассылка писем с вымогательством денежных средств за прекращение атак;
- маркеры заражения вредоносным программным обеспечением (например, временные папки, хеш-суммы файлов, создаваемые сетевые соединения и процессы);
- управляющие команды, которые могут быть использованы для удаленного несанкционированного управления программным обеспечением;
- IP-адреса и доменные имена сайтов, используемых для осуществления мошеннических действий;
- телефонные номера, с которых осуществляются мошеннические SMS-рассылки и телефонные звонки.

По мере необходимости работники Центра в рамках своих полномочий принимают участие в совместной с правоохранительными органами работе по определению IP-адресов, с которых осуществлялись DDoS-атаки, привлекаются в качестве консультантов и специалистов в области безопасности банковских технологий.

Рекомендации кредитным организациям для повышения безопасности

Необходимо соблюдать ряд правил:

Разделять сегменты локальной вычислительной сети кредитной организации, в которых обрабатывается платежная и иная информация, с обязательным контролем входящих и исходящих потоков данных.

Использовать эшелонированную и своевременно обновляемую защиту. При этом средства защиты информации должны быть не просто установлены в инфраструктуре, но и в обязательном порядке настроены с учетом особенностей бизнес-процессов кредитной организации.


Рассчитывать риски нарушения информационной безопасности и включать их в состав операционных рисков кредитной организации.

Повышать квалификацию работников служб информационной безопасности.

Участие специалистов кредитной организации в непрерывном взаимном информировании об угрозах нарушения информационной безопасности, организованном Центром, и понимание на уровне руководства кредитной организации важности подобного обмена.

Источник: Журнал "Information Security/ Информационная безопасность" #1, 2016

Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT)

← Я ↻  www.cbr.ru Информация по кредитным организациям | Банк России



Центральный банк
Российской Федерации

Весь сайт + [Информация по кредитным организациям](#) + [Информационная безопасность организаций банковской системы Российской Федерации](#)

RU EN

«ФинЦЕРТ» Банка России

Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере — структурное подразделение Главного управления безопасности и защиты информации Банка России.

PDF [Типовая форма соглашения о взаимодействии Центрального банка Российской Федерации по вопросам противодействия компьютерным атакам](#)

PDF [Обзор несанкционированных переводов денежных средств за 2016 год](#)

PDF [Отчет Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления безопасности и защиты информации Банка России за период с 01 июня 2015 г. по 31 мая 2016 г.](#)

PDF [Временный регламент передачи данных участников информационного обмена в Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России \(версия 1.0\)](#)

[Информация по кредитным организациям](#)

[Информационная безопасность организаций банковской системы Российской Федерации](#)

[Стандарты Банка России](#)

[Рекомендации в области стандартизации](#)

«ФинЦЕРТ» Банка России

Основная цель

Создание центра компетенции в рамках информационного взаимодействия Банка России, кредитных и некредитных финансовых организаций, компаний-интеграторов, разработчиков антивирусного программного обеспечения, провайдеров и операторов связи, а также для правоохранительных и иных государственных органов, курирующих информационную безопасность отрасли. Указанное информационное взаимодействие направлено на координацию работ по противодействию злоумышленникам, активность которых направлена на личное обогащение с использованием методов несанкционированного доступа к ИТ-инфраструктуре организаций, поднадзорных Банку России, а также с использованием уязвимостей в платежных технологиях.

Для достижения цели выполняются следующие задачи:

- Организация и координация обмена информацией Центра, правоохранительных органов, кредитных и некредитных финансовых организаций
- Анализ данных о фактах компьютерных атак в кредитных и некредитных финансовых организациях и подготовка аналитических материалов
- Установление рекомендаций в области обеспечения защиты информации при осуществлении переводов денежных средств.

Информационный обмен

Участником информационного обмена может стать любое юридическое лицо, которое:

- Осуществляет финансовую деятельность и зарегистрировано в установленном порядке в Центральном Банке Российской Федерации (имеет соответствующую лицензию)
- Является производителем средств программного и аппаратного обеспечения в области защиты информации
- Выполняет иные работы в области защиты информации, преимущественно в кредитно-финансовой сфере

Участие добровольное. Для того чтобы принять участие в информационном обмене, заполните [«Карточку участника»](#) и отправьте запрос на электронный адрес info_fincert@cbr.ru с пометкой **«Информационное взаимодействие»**.

Поля «Карточки участника» заполняются согласно вашим возможностям. В контактах ответственных лиц следует указать адрес электронной почты и телефон для связи.

По любым возникающим вопросам можно связаться с работниками Центра:

Телефон: +7 (495) 772-70-90

E-mail: info_fincert@cbr.ru

Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT)

www.cbr.ru survey_transfers_16.pdf

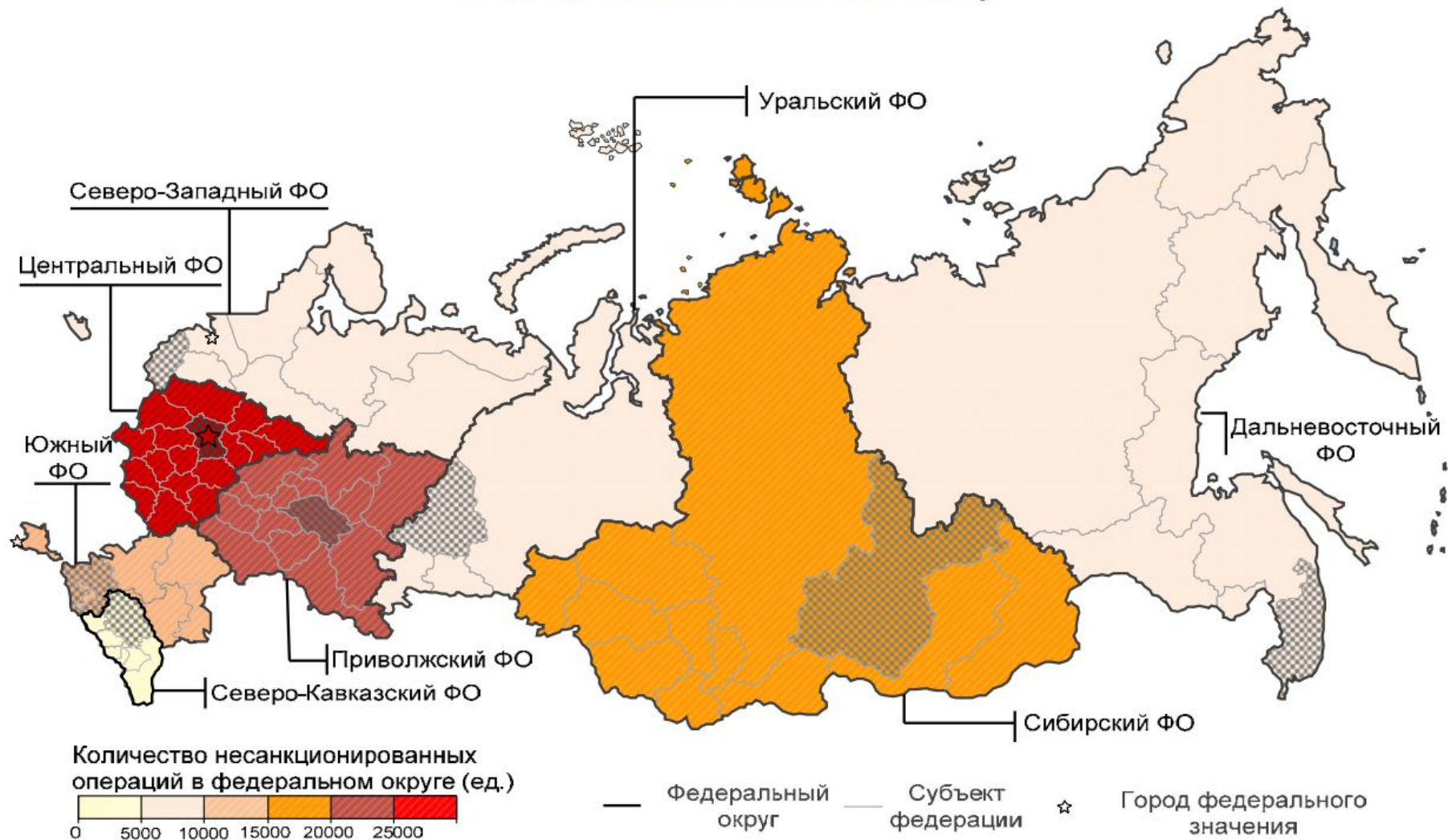
Сохранить Напечатать



ОБЗОР НЕСАНКЦИОНИРОВАННЫХ
ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ
ЗА 2016 ГОД

Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT)

Территориальное распределение несанкционированных операций с использованием платежных карт



Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT)

Рост кибератак на кредитно-финансовые организации очевиден. Для эффективной борьбы с ними Банк России создал Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT), который осуществляет сбор и анализ информации от финансовых учреждений о кибератаках, а также предупреждает о возможных угрозах ИБ и взаимодействует с правоохранительными органами.



FINCERT. НАПРАВЛЕНИЯ РАЗВИТИЯ

3

Создание

- По поручению Совета Безопасности РФ в структуре ГУБиЗИ Банка России сформирован Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT).

Цель

- Создание единой и доверенной информационной среды для эффективного противодействия кибермошенничеству и киберпреступлениям на объектах кредитно-финансовой сферы.

Задачи

- Организация и координация обмена информацией с правоохранительными органами и КО;
- Мониторинг, реагирование и анализ данных о фактах компьютерных атак, подготовка аналитических материалов;
- Установление рекомендаций в области обеспечения защиты информации.

Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT)



ФИНЦЕРТ. ВЗГЛЯД ИЗНУТРИ

Получение исходных данных

3



Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT)

Обращение

Краткое содержание*

Текст обращения*

Количество символов не должно превышать 15000.

Название кредитной или иной организации, с деятельностью которой связано Ваше обращение

Для поиска названия кредитной организации воспользуйтесь Справочником по кредитным организациям

Выбор региона адресата*

Направление обращений граждан на рассмотрение в подразделения Банка России осуществляется в соответствии с организационной структурой Банка России

Выбор файлов

Загрузка файлов пользователя

Перетащите файлы в это поле (drag & drop)

Фрагмент формы обращения на сайте Банка России

Самый предпочтительный вариант взаимодействия с FinCERT - по электронной почте, так как он будет самым оперативным. В этом случае, как заявляют представители Центра, время на обработку входящего сообщения займет 1 рабочий день или около того. Попытка достучаться до FinCERT по официальным каналам (через территориальные управления или через Интернет-приемную) затянут ответ на несколько недель. Бюрократия - это то, что может убить центр мониторинга и реагирования на инциденты, который должен функционировать более оперативно, чем это принято сейчас в госорганах.

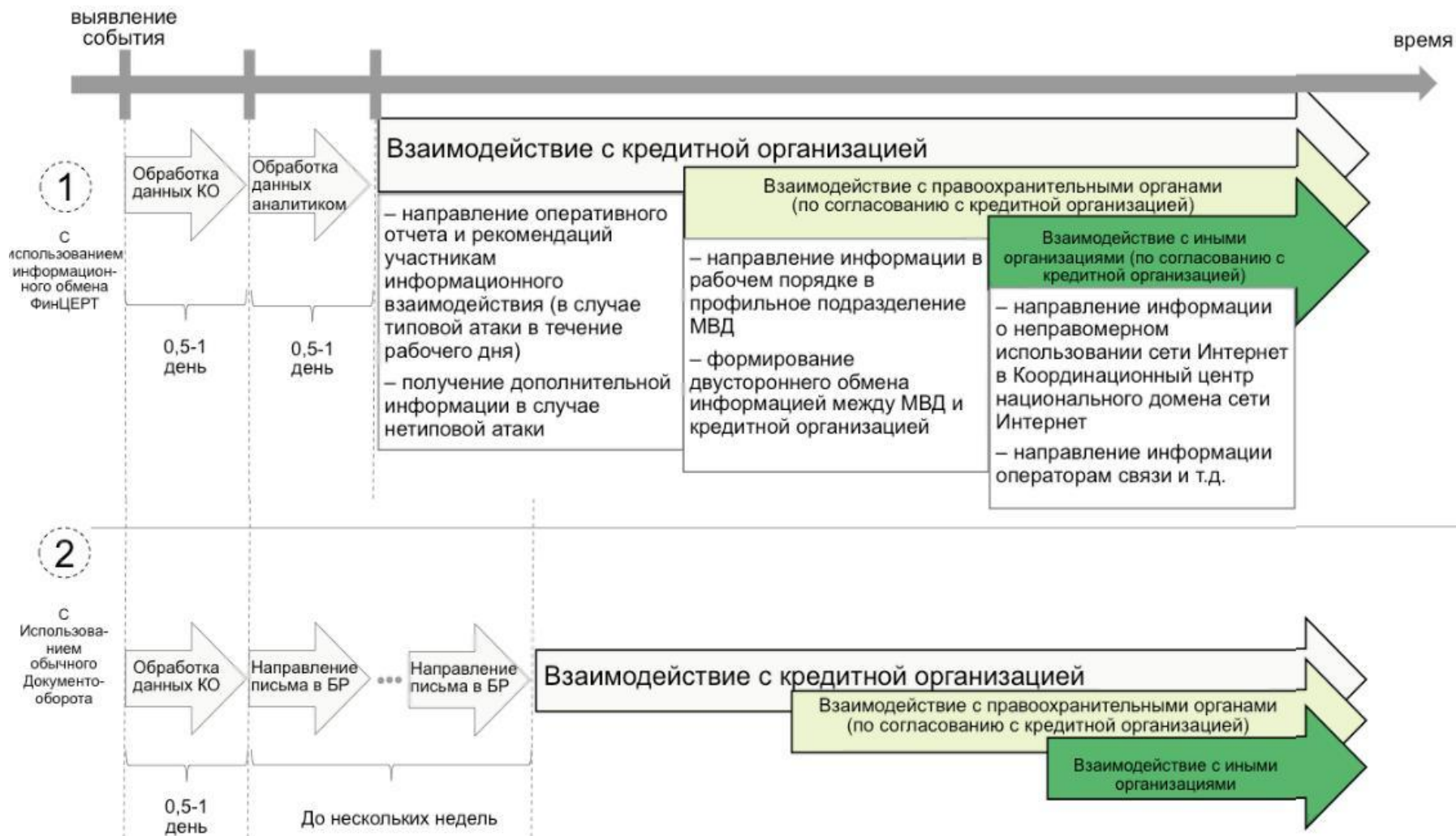
Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT)



ФИНЦЕРТ. ВЗГЛЯД ИЗНУТРИ

Рассмотрение обращения, подготовка оперативных отчетов и рекомендаций

5



Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT)



FINCERT. НАПРАВЛЕНИЯ РАЗВИТИЯ



Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT)



Общая схема работы



Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT)



Работа аналитиков

Аналитика вредоносного программного обеспечения

экземпляр вредоносного ПО

- Определение детектируемости антивирусными программными средствами по данным VirusTotal
- Определение маркеров заражения

Техническая аналитика

лог-файлы и образы дисков

- Выявление нестандартной сетевой активности
- Выявление нестандартных действий локальных пользователей

Аналитика бизнес-процессов

бизнес-процессы

- Сопоставление существующих бизнес-процессов и полученных в результате технической аналитики данных



Методологическое обеспечение деятельности FinCERT



Центр мониторинга и реагирования на компьютерные атаки VI.ZONE (Сбербанк)

В марте 2016 году Сбербанк основал дочернюю компанию «Безопасная информационная зона» (краткое название – «Бизон»), ведущую деятельность в области ИБ. Ее задачами является анализ ситуации в мире в области киберугроз, тестирование всех систем Сбербанка на предмет их уязвимости, а также экспертиза, связанная с киберрисками. Данная компания также оказывает поддержку для работы единого операционного центра информационной безопасности (Security Operation Center, SOC) Сбербанка.

В задачи "Бизон" входит тестирование систем Сбербанка на предмет их уязвимости, а также экспертиза, связанная с киберрисками. "Бизон" работает в партнерстве с банками и страховыми компаниями. Компания специализируется на выявлении случаев фишинга и нарушений прав финансово-кредитных организаций.

Планируется с 2016 г., что «Бизон» получит право блокировать фишинговые сайты

Координационный центр национального домена сети интернет (КЦ) может предоставить "Бизон" право делегировать (выключать) сайты, если через них осуществляется кража паролей или денег.

Для передачи "Бизону" таких прав КЦ намерен воспользоваться пунктом 5.7 "Правил регистрации доменных имен в зоне .ru и ".рф", где говорится, что регистратор вправе прекратить делегирование домена, который используется для фишинга, распространения вирусов или материалов с детской порнографией". В данном случае "Бизон" будет выступать в роли "компетентной организации", определяющей, какой домен следует деактивировать.

В России борьбу с запрещенной и опасной информацией в сети интернет параллельно осуществляют несколько ведомств. Выявлением порнографических материалов занимается Роскомнадзор, поиском информации по незаконному распространению наркотиков и их пропаганде - МВД, обнаружением материалов с пропагандой суицида и выявлением информации, вредной для здоровья детей, - Роспотребнадзор. Федеральная налоговая служба занимается азартными играми, а Генпрокуратура выявляет в интернете экстремистские материалы. При этом делегирование домена может быть прекращено либо Управлением "К" МВД, либо Генпрокуратурой.

Центр мониторинга и реагирования на компьютерные атаки VI.ZONE (Сбербанк)

Координационный центр национального домена сети Интернет

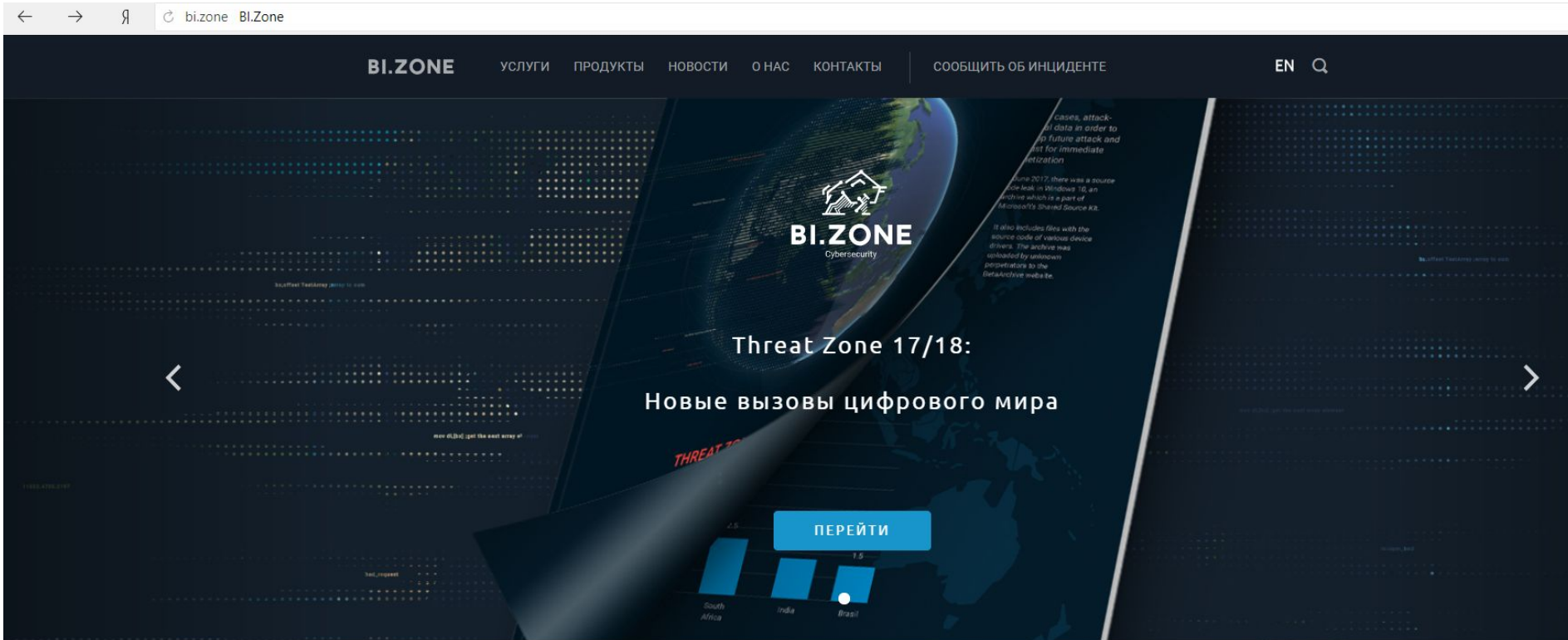
Правила регистрации доменных имен в доменах .RU и .РФ

Индекс документа	Редакция от 03.12.2015	Утвержден решением № 2011-18/81 от 05.10.2011	Дата начала действия документа ___.20__
Статус документа обязательный		Отменен (изменен) решением № 2015-09/60 от 03.12.2015	Дата окончания действия

Правила регистрации доменных имен в доменах .RU и .РФ (именуемые в дальнейшем «Правила») регулируют отношения, возникающие в связи с регистрацией доменных имен второго уровня в доменах .RU и .РФ.

Настоящие Правила не распространяются на отношения, связанные с содержанием и/или распространением информации, адресуемой с помощью доменных имен.

Центр мониторинга и реагирования на компьютерные атаки BI.ZONE (Сбербанк)



Круглосуточная помощь от Центра оперативного реагирования

СООБЩИТЬ ОБ ИНЦИДЕНТЕ

Центр мониторинга и реагирования на компьютерные атаки BI.ZONE (Сбербанк)

bi.zone BI.Zone

BI.ZONE

УСЛУГИ

ПРОДУКТЫ

НОВОСТИ

О НАС

КОНТАКТЫ

СООБЩИТЬ ОБ ИНЦИДЕНТЕ

EN 

УСЛУГИ

Проактивная защита



Защита бренда



Тестирование на защищённость
от методов социальной инженерии



Сбор информации о потенциальных
угрозах

Компьютерная криминалистика



Реагирование на инциденты



Расследование инцидентов
кибербезопасности



Исследование и анализ
вредоносного программного
обеспечения

Тестирование периметра



Нагрузочное и
функциональное
тестирование



Регулярное сканирование
внешнего периметра



Тестирование
на проникновение



Тестирование
защищённости
мобильных и веб-
приложений

Центр мониторинга и реагирования на компьютерные атаки BI.ZONE (Сбербанк)

bi.zone BI.Zone

BI.ZONE УСЛУГИ ПРОДУКТЫ НОВОСТИ О НАС КОНТАКТЫ СООБЩИТЬ ОБ ИНЦИДЕНТЕ EN Q

НОВОСТИ

[Все новости](#)

26 Октября 2018

Компания BI.ZONE приняла участие в конференции Sibos 2018

С 22 по 25 октября в Сиднее, Австралия, состоялась очередная конференция Sibos, организованная компанией SWIFT. Участники мероприятия в Сиднее обсудили проблемы кибербезопасности, с которыми сталкиваются в ежедневной работе, и особенно подчеркнули важность укрепления сотрудничества в области противодействия киберугрозам на международном уровне.

[Читать подробнее...](#)

8 Октября 2018

В ноябре BI.ZONE проведет конференцию OFFZONE 2018

15–16 ноября 2018 года в Москве состоится международная конференция по кибербезопасности OFFZONE 2018, которая пройдет в центре Digital October и объединит на своей площадке экспертов, исследователей, участников профессионального комьюнити и всех неравнодушных к миру практической кибербезопасности.

[Читать подробнее...](#)

9 Июля 2018

BI.ZONE заключил соглашения с новыми партнерами в рамках ICC 2018

Компания BI.ZONE приняла участие в Международном конгрессе по кибербезопасности. В рамках конгресса компания BI.ZONE и технологический проект Vostok заключили меморандум о взаимопонимании.

[Читать подробнее...](#)

1/7

Компьютерная криминалистика

- Исследование и анализ вредоносного программного обеспечения
- Расследование инцидентов кибербезопасности
- Реагирование на инциденты

Проактивная защита

- Сбор информации о потенциальных угрозах
- Тестирование на защищенность от методов социальной инженерии
- Защита бренда

Тестирование периметра

- Тестирование защищенности мобильных и веб-приложений
- Тестирование на проникновение
- Регулярное сканирование внешнего периметра
- Нагрузочное и функциональное тестирование

Продукты

- TI Platform
- BI.ZONE Cloud Fraud Prevention

О нас

- О компании
- Вакансии
- Новости
- Контакты



Круглосуточная линия

+7 499 110 25 34

info@bi.zone
cert@bi.zone

[СООБЩИТЬ ОБ ИНЦИДЕНТЕ](#)

↑

© 2018 BI.ZONE  BI.ZONE на Хабре 

Центр мониторинга и реагирования на компьютерные атаки BI.ZONE (Сбербанк)

BI.ZONE

УСЛУГИ

ПРОДУКТЫ

НОВОСТИ

О НАС

КОНТАКТЫ

СООБЩИТЬ ОБ ИНЦИДЕНТЕ

EN 

Продукты

Fraud Prevention



BI.ZONE Cloud Fraud Prevention

Облачное кросс-канальное решение для выявления мошеннических операций в онлайн-каналах платежей в режиме реального времени.

[ПОДРОБНЕЕ](#)

Threat intelligence



TI.Platform

Платформа для непрерывной агрегации, верификации и обогащения данных об актуальных угрозах кибербезопасности.

[ПОДРОБНЕЕ](#)

ЗАКАЗАТЬ РАСЧЕТ СТОИМОСТИ УСЛУГ

Название организации

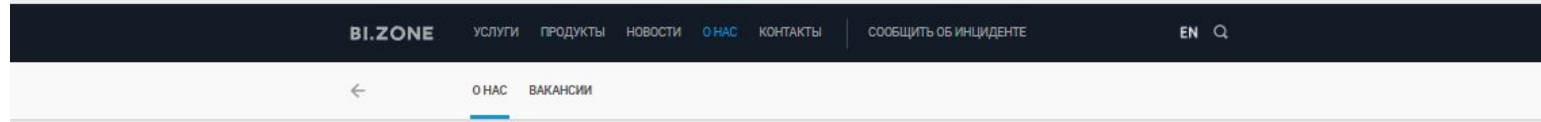
ФИО контактного лица

Телефон

E-mail

Опишите подробности

Центр мониторинга и реагирования на компьютерные атаки BI.ZONE (Сбербанк)



О нас

BI.ZONE – визионер российского рынка кибербезопасности, предлагающий услуги по защите активов и репутации бизнеса в сети Интернет, основанные на киберразведке и постоянном мониторинге информационных потоков в публичных и теневых сегментах киберпространства.

Сочетание уникальной экспертизы и передовых технологий в области практической кибербезопасности для эффективной защиты самых ценных активов бизнеса и государственных организаций.

BI.ZONE – уверенный игрок на рынке кибербезопасности, который способен ощутимо снизить риск сетевых атак и несанкционированного доступа к чувствительной информации заказчика.

ЗАКАЗАТЬ РАСЧЕТ СТОИМОСТИ УСЛУГ

Название организации

ФИО контактного лица

Телефон

E-mail

Опишите подробности

Отправляя форму, я даю согласие на обработку своих персональных данных в соответствии с Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ. Я понимаю и соглашусь, что мои данные будут храниться и обрабатываться в ООО «БИЗон» в течение десяти лет в соответствии с Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ.

ЗАКАЗАТЬ

Центр мониторинга и реагирования на компьютерные атаки BI.ZONE (Сбербанк)

bi.zone Контакты

BI.ZONE

УСЛУГИ

ПРОДУКТЫ

НОВОСТИ

О НАС

КОНТАКТЫ

СООБЩИТЬ ОБ ИНЦИДЕНТЕ

EN Q

Контакты

Круглосуточная линия

+7 499 110 25 34

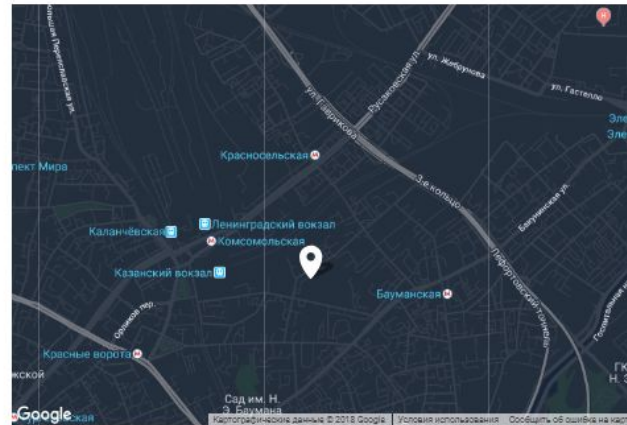
Электронная почта

info@bi.zone

cert@bi.zone

Адрес офиса

105066, г. Москва, улица Ольховская, дом 4, корпус 2



ЗАКАЗАТЬ РАСЧЕТ СТОИМОСТИ УСЛУГ

Название организации

ФИО контактного лица

Телефон

+7 123 456 78 90

Центр мониторинга и реагирования на компьютерные атаки BI.ZONE (Сбербанк)

О НАС **ВАКАНСИИ**

Кто мы такие?

BI.ZONE занимается кибербезопасностью — защитой данных, активов и репутации. Мы собрали у себя профессионалов своего дела и лучших экспертов кибербезопасности — разработчиков, тестировщиков, инженеров и т.д.

Кого мы ищем?

Мы ищем не просто профессионалов, а еще и единомышленников. У нас много интересных и сложных задач, и мы высоко ценим людей, которые могут эти задачи решить.

Вакансии

[Специалист Network Security](#)

[Front-end разработчик \(React.js\)](#)

[Ведущий специалист по тестированию \(клиентское направление\)](#)

[Ведущий специалист по тестированию \(интеграционное направление\)](#)

[Lead Go \(Golang\) разработчик](#)

[Ведущий инженер по информационной безопасности](#)

от 120000 руб.

[Ведущий специалист по нагрузочному тестированию BigData и Highload](#)

[Разработчик C](#)

[Scala разработчик \(Senior\)](#)

[Специалист DevOps](#)

[Специалист Endpoint Security](#)

[Аналитик](#)

[Разработчик JavaScript](#)

[Специалист сопровождения облачного сервиса](#)

[Администратор облачных сервисов](#)

[Системный администратор](#)

[Системный инженер по системам анализа и обработки данных в реальном времени](#)

от 120000 руб.

[Проектный инженер отдела тестирования и анализа средств защиты информации](#)

[Технический консультант направления тестирования и мониторинга](#)

[Аналитик отдела ИТ](#)

[Посмотреть остальные 2 вакансии на hh.ru](#)



Почему надо к нам идти?

Можно было бы написать про «молодой дружный коллектив», но не будем (хотя он и правда молодой и довольно дружный).

У нас:

- Высокопрофессиональный коллектив — есть у кого поучиться;
- Высокая зарплата;
- Адекватное и всегда доступное для диалога руководство;
- Полностью «белое» оформление;
- Работа в центре Москвы (м. Комсомольская) — не бездушный опенспейс, а уютный и ламповый офис с отдельными кабинетами у каждой из команд;
- Возможность учиться и развиваться — компенсация обучения и конференций;
- Удобный офис с душем, велопарковкой, кофе-чаем, фруктами и завтраками.

Как с нами связаться?

Отправьте резюме нашему HR-директору Марине Смоленковой по адресу m@bi.zone, hr@bi.zone или откликнитесь на одну из вакансий из списка выше. Если ни одна из вакансий вам точно не подходит, но вы все-таки хотите к нам — не стесняйтесь! Просто заполните форму ниже и расскажите о себе и своих талантах.

ОТПРАВИТЬ ЗАЯВКУ НА СОТРУДНИЧЕСТВО

Направление деятельности

ФИО контактного лица

Перспективы развития системы Центров реагирования на компьютерные инциденты в России

В ближайшее время в России в полную силу заработает центр реагирования на инциденты в сфере информационной безопасности (CERT), созданный "Лабораторией Касперского" для сбора информации об уязвимостях и отражении атак на такие объекты, как атомные электростанции, предприятия ядерно-топливного, нефтегазового и энергетического комплексов.

Обезопасить свою инфраструктуру намерены и телекоммуникационные операторы, которые ведут переговоры с Минкомсвязью и ФСБ о создании соответствующего CERT.

Россия перенимает опыт США, где есть свои CERT в каждой важной отрасли. Но при этом не факт, что крупнейшие корпорации захотят делиться с "Лабораторией Касперского" информацией об уязвимости своей критической инфраструктуры.

"Лаборатория Касперского" намерена в октябре запустить CERT на критически важных объектах и информационной инфраструктуре (КИИ), таких как атомные электростанции, предприятия ядерно-топливного, нефтегазового, энергетического и оборонного комплексов, металлургические и химические производства. В настоящий момент "Лаборатория Касперского" плотно работает с отраслевыми и государственными регуляторами и организациями, отвечающими за обеспечение кибербезопасности не только в России, но и по всему миру", — руководитель центра компетенции по защите критической инфраструктуры "Лаборатории Касперского" Евгений Гончаров. CERT будет собирать информацию о найденных уязвимостях, угрозах, инцидентах, а также привлекаться к проведению обследований, тестов на проникновение и расследований инцидентов на промышленных объектах.

CERT планируется сделать международным и в ближайшее время получить от Университета Карнеги-Меллон право на использование торговой марки CERT, которую университет дает центрам реагирования на киберинциденты по всему миру.

Перспективы развития системы Центров реагирования на компьютерные инциденты в России

Безопасностью критически важных объектов в России занимаются сразу несколько организаций, в основном ФСТЭК и ФСБ.

В январе 2013 года Владимир Путин подписал указ о создании в России системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы (ГосСОПКА), организацию работ по созданию которой поручил ФСБ.

В список задач ГосСОПКА входит оценка степени защищенности КИИ от компьютерных атак и установление причин таких инцидентов.

Промышленный CERT "Лаборатории Касперского" наверняка будет работать в связке с ГосСОПКА и получать информацию об инцидентах и атаках на промышленные объекты именно от госсистемы. "Но предприятия уровня "Газпрома", "Роснефти" и подобных не будут частной компании добровольно отдавать информацию о своих уязвимостях",— считает эксперты.

В пресс-службе "РусГидро" сообщили, что компания активно работает в направлении создания своего корпоративного центра по управлению ИБ (SOC) и по организации взаимодействия с ГосСОПКА. "Тот функционал, который предлагает в данный момент "Лаборатория Касперского", мы планируем реализовывать самостоятельно в прямом сотрудничестве с ФСБ",— говорят в компании.

В "Лаборатории Касперского" отмечают, что "открыты к взаимодействию со всеми организациями или структурами и ГосСОПКА не исключение".

В настоящее время вопрос создания еще одного CERT — для реагирования на инциденты на телекоммуникационных сетях — обсуждается и между федеральными операторами связи, Минкомсвязью и ФСБ. Вопрос создания CERT для защиты инфраструктуры телеком-операторов уже поднимался несколько лет назад. Минкомсвязь тогда посчитала, что вопросы информационной безопасности на телеком-инфраструктуре не являются ее сферой деятельности, а Роскомнадзор, на базе ситуационного центра которого предлагали создать такую структуру, идею не поддержал. Операторам было непросто договориться между собой, потому что для обеспечения информбезопасности у них есть свои SOC. Вопрос создания Telecom-CERT был поднят снова, когда начались обсуждения необходимости обеспечения целостности и безопасности российского сегмента интернета и "в связи с увеличением количества и качества информационных угроз".

Перспективы развития системы Центров реагирования на компьютерные инциденты в России

В России уже работает несколько государственных и частных CERT.

RU-CERT, созданный НИИ развития общественных сетей, и CERT-GIB, который принадлежит компании Group-IB, занимаются снижением уровня ИБ-угроз для пользователей рунета.

Созданный ФСБ GOV-CERT.RU направлен на повышение защищенности органов власти, а FinCERT, основанный ЦБ, собирает информацию о кибератаках на финансовые учреждения.

В Японии и США есть центры разбора ИБ-инцидентов в наиболее важных индустриях: финансовом секторе, телекоммуникациях, медицине и др. Для инцидентов на промышленных объектах, например, в США работает ICS-CERT. Россия пытается идти по тому же пути. В силу развитой и распределенной IT-инфраструктуры телеком-операторы подвергаются тысячам атак ежедневно. В 90% случаев это массовые ненаправленные атаки, когда заражаются компьютеры и серверы телеком-оператора с целью формирования бот-сети. Атаки на промышленные предприятия меньше в масштабах, но потенциальный ущерб от успешной атаки на КИИ предприятия может затрагивать вопросы жизнеобеспечения граждан.

Вопрос 4

**Федеральные государственные органы РФ,
осуществляющие полномочия по предотвращению
противоправных действий и борьбе
с преступлениями в сфере компьютерной информации**

Классификация компьютерных преступлений и преступлений, совершаемых с использованием новых информационных технологий

Несмотря на многообразие компьютерных преступлений, практически все способы их совершения имеют свои индивидуальные, присущие только им признаки, по которым их можно распознать и классифицировать по отдельным общим группам:

1. Изъятие средств компьютерной техники.
2. Неправомерный доступ к компьютерной информации:
 - Преступления, совершаемые в отношении компьютерной информации, находящейся в компьютерах и глобальных компьютерных сетях или при обращении к ним.
 - Преступления, совершаемые в отношении компьютерной информации, находящейся в ЭВМ, не являющихся компьютером в классическом понимании этого слова (таких, как сервер, сотовый телефон, кассовый аппарат и т.п).
3. Изготовление или распространение вредоносных программ (вирусы, программы - взломщики и т.п.).
4. Перехват информации.
5. Нарушение авторских прав (компьютерное пиратство).
6. Мошенничество с использованием платежных карт.
7. Преступления, совершаемые с использованием информационно-телекоммуникационных сетей, в том числе сети "Интернет", а также средств связи, в том числе подвижной связи.

Федеральные государственные органы РФ, осуществляющие полномочия по предотвращению противоправных действий и борьбе с преступлениями в сфере компьютерной информации

Федеральный закон от 28.12.2010 N 403-ФЗ (ред. от 28.12.2016) "О Следственном комитете Российской Федерации"

...

4. Основными задачами Следственного комитета являются:

- 1) оперативное и качественное расследование преступлений в соответствии с подследственностью, установленной уголовно-процессуальным законодательством Российской Федерации;
- 2) обеспечение законности при приеме, регистрации, проверке сообщений о преступлениях, возбуждении уголовных дел, производстве предварительного расследования, а также защита прав и свобод человека и гражданина;

...

- 4) организация и осуществление в пределах своих полномочий выявления обстоятельств, способствующих совершению преступлений, принятие мер по устранению таких обстоятельств;

...

Федеральный закон от 07.02.2011 N 3-ФЗ "О полиции".

...

Статья 2. Основные направления деятельности полиции

1. Деятельность полиции осуществляется по следующим основным направлениям:

- 1) защита личности, общества, государства от противоправных посягательств;
- 2) предупреждение и пресечение преступлений и административных правонарушений;
- 3) выявление и раскрытие преступлений, производство дознания по уголовным делам;

...

- 5) производство по делам об административных правонарушениях, исполнение административных наказаний;

...

Раздел VII. ПРЕСТУПЛЕНИЯ ПРОТИВ ЛИЧНОСТИ

Глава 19. Преступления против конституционных прав и свобод человека и гражданина

Статья 137. Нарушение неприкосновенности частной жизни

Статья 138. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений

Статья 138.1. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации

Статья 146. Нарушение авторских и смежных прав

Статья 147. Нарушение изобретательских и патентных прав

РАЗДЕЛ VIII. ПРЕСТУПЛЕНИЯ В СФЕРЕ ЭКОНОМИКИ

ГЛАВА 21. Преступления против собственности

Статья 159. Мошенничество

Статья 159.3. Мошенничество с использованием платежных карт

Статья 159.6. Мошенничество в сфере компьютерной информации

Глава 22. Преступления в сфере экономической деятельности

Статья 171.2. Незаконная организация и проведение азартных игр

Статья 185.3. Манипулирование рынком

Статья 185.6. Неправомерное использование инсайдерской информации

Статья 187. Изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов

РАЗДЕЛ VIII. ПРЕСТУПЛЕНИЯ ПРОТИВ ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ И ОБЩЕСТВЕННОГО ПОРЯДКА

Глава 25. Преступления против здоровья населения и общественной нравственности

Статья 228.1. Незаконное производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества

Статья 242. Незаконное изготовление и оборот порнографических материалов или предметов

Статья 242.1. Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних

Статья 242.2. Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов

Глава 28. Преступления в сфере компьютерной информации

Статья 272. Неправомерный доступ к компьютерной информации

Статья 273. Создание, использование и распространение вредоносных компьютерных программ

Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

Раздел X. ПРЕСТУПЛЕНИЯ ПРОТИВ ГОСУДАРСТВЕННОЙ ВЛАСТИ

Глава 29. Преступления против основ конституционного строя и безопасности государства

Статья 280. Публичные призывы к осуществлению экстремистской деятельности

Статья 280.1. Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации

Статья 282. Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства

Назначение уголовного судопроизводства

Уголовное судопроизводство в широком смысле – урегулированная нормами уголовно-процессуального права деятельность органов дознания, следователей, прокуроров и судов по уголовным делам о преступлениях, то есть деятельность по возбуждению уголовного дела, его расследованию, судебному разбирательству, вынесению приговора (иного решения по делу), пересмотру решения в вышестоящих судах, исполнению вступившего в законную силу судебного решения.

В узком смысле – только стадия судебного разбирательства.

Назначение:

- защита прав и законных интересов лиц и организаций, потерпевших от преступлений.
- защита личности от незаконного и необоснованного обвинения, осуждения, ограничения прав и свобод.
- уголовное преследование и назначение справедливого наказания.
- отказ от уголовного преследования невиновных лиц, освобождение их от наказания.
- реабилитация лиц, незаконно подвергшихся уголовному преследованию.

Досудебное производство состоит из следующих стадий:

- возбуждение уголовного дела. Ее основная задача – обеспечить быстрое реагирование на каждое преступление и создать возможность для всестороннего, полного и объективного исследования всех обстоятельств происшедшего.
- предварительное расследование. Задачи: а) быстрое и полное раскрытие преступления; б) обличение виновных путем сбора достаточного количества доказательств; в) выявление причин и условий, способствовавших совершению преступления; г) принятие мер по обеспечению возмещения материального ущерба (розыск и изъятие похищенного и т. д.).

Судебное производство по уголовному делу включает в себя следующие стадии:

подготовка к судебному заседанию; судебное разбирательство в суде первой инстанции; апелляционное производство; исполнение приговора; кассационное производство; надзорное производство; возобновление производства по уголовному делу ввиду новых или вновь открывшихся обстоятельств.

"Уголовно-процессуальный кодекс Российской Федерации" от 18.12.2001 N 174-ФЗ (ред. от 03.04.2017)

Ст. 150. Формы предварительного расследования

1. Предварительное расследование производится в форме предварительного следствия* либо в форме дознания**.

2. Производство предварительного следствия обязательно по всем уголовным делам, за исключением уголовных дел о преступлениях, указанных в части третьей настоящей статьи***.

3. Дознание производится:

1) по уголовным делам о преступлениях, предусмотренных статьями ... ****

Дознание – это форма расследования преимущественно преступлений небольшой тяжести (умышленные и неосторожные деяния; ≤ 3 лет лишения свободы) либо средней тяжести (умышл. д.; ≤ 5 лет; неостор. д. ≥ 3 лет). По результатам проверки составляется обвинительное заключение, которое утверждается начальником органа дознания или прокурором.

Предварительное следствие – это форма расследования преступлений, перечисленных в ч.2 ст.151 УПК РФ (как правило, тяжких (умышл. д.; ≤ 10 лет) и особо тяжких(умышл. д.; ≥ 10 лет), проводимая в случаях, когда подозреваемый не установлен. По результатам расследования составляется обвинительное заключение.

Важнейшие отличия:

- составы уголовно-наказуемых деяний и наличие виновного лица. Дознаватели могут расследовать лишь те преступления, которые перечислены в ч.3 ст.151 УПК РФ и по которым имеется подозреваемый, в то время как следователи – любые, помимо тех, что указаны в ч.2 ст.151 УПК РФ.

- итоги. По результатам предварительного расследования составляется обвинительное заключение, по результатам дознания – обвинительный акт.

- сроки проведения. Предварительное следствие должно быть завершено в срок до 2 месяцев, дознание – до 20 дней.

- продление сроков. Срок следствия может продлеваться до 6 месяцев (прокурорами района, города), до 1 года (прокурором субъекта РФ), и более (Генеральным прокурором). Дознание продлевается максимум на 10 суток.

- субъект. Предварительное следствие проводится следователями СК, ОВД, ФСБ, дознание – дознавателями ОВД, ФССП, ГПН.

Примечание автора: * Осуществляется следователями СК, ФСБ, ОВД

** Осуществляется дознавателями ОВД, пограничных органов ФСБ, органов ФССП, органов гос. пож. надзора фед. пож. службы, следователями СК, дознавателями тамож. органов РФ

***По этим статьям проводится дознание

****В частности, статьями, связанными с преступлениями в сфере ИТ, такими как, 159.3 частью первой, 159.6 частью первой, 228 частью первой, 242.

"Уголовно-процессуальный кодекс Российской Федерации" от 18.12.2001 N 174-ФЗ (ред. от 03.04.2017)

Статья 151. Подследственность

1. Предварительное расследование производится следователями и дознавателями.

2. Предварительное следствие производится:

1) следователями Следственного комитета Российской Федерации - по уголовным делам:

а) о преступлениях, предусмотренных статьями 105 - 110, 111 частью четвертой, 120, 126, 127 частями второй и третьей, 127.1 частями второй и третьей, 127.2 частями второй и третьей, 128, 131 - 149, 169, 170.1, 171.2, 172.1, 185 - 185.6, 194 частями третьей и четвертой, 198 - 199.2, 201, 204, 204.1, 205 - 205.2, 205.3, 205.4, 205.5, 208 - 212.1, 215, 215.1, 216 - 217.2, 227, 235.1, 237, 238, 238.1, 239, 240.1, 242.1, 242.2, 246 - 249, 250 частями второй и третьей, 251 частями второй и третьей, 252 частями второй и третьей, 254 частями второй и третьей, 255, 258.1 частями второй и третьей, 263, 263.1, 269, 270, 271, 271.1, 279, 282 - 282.3, 284.1, 285 - 291.1, 292 - 293, 294 частями второй и третьей, 295, 296, 298.1 - 305, 317, 318, 320, 321, 327.2, 328, 330.1, 330.2, 332 - 354.1 и 356 - 361 Уголовного кодекса Российской Федерации;

б) о преступлениях, совершенных лицами, указанными в статье 447 настоящего Кодекса, за исключением случаев, предусмотренных пунктом 7 части третьей настоящей статьи, а также о преступлениях, совершенных в отношении указанных лиц в связи с их профессиональной деятельностью;

в) о преступлениях, совершенных должностными лицами Следственного комитета Российской Федерации, органов федеральной службы безопасности, Службы внешней разведки Российской Федерации, Федеральной службы охраны Российской Федерации, органов внутренних дел Российской Федерации, учреждений и органов уголовно-исполнительной системы, таможенных органов Российской Федерации, военнослужащими и гражданами, проходящими военные сборы, лицами гражданского персонала Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов в связи с исполнением ими своих служебных обязанностей или совершенных в расположении части, соединения, учреждения, гарнизона, за исключением случаев, предусмотренных пунктом 7 части третьей настоящей статьи, а также о преступлениях, совершенных в отношении указанных лиц в связи с их служебной деятельностью;

г) о тяжких и особо тяжких преступлениях, совершенных несовершеннолетними и в отношении несовершеннолетних;

"Уголовно-процессуальный кодекс Российской Федерации" от 18.12.2001 N 174-ФЗ (ред. от 03.04.2017)

Статья 151. Подследственность

2. Предварительное следствие производится: (продолжение)

2) следователями органов федеральной службы безопасности - по уголовным делам о преступлениях, предусмотренных статьями 189, 200.1 частью второй, 205, 205.1, 205.2, 205.3, 205.4, 205.5, 208, 211, 215.4 частью второй пунктом "б", 217.1, 226.1, 229.1, **275 - 281**, 283, 283.1, 284, 322 частью третьей, 322.1 частью второй, 323 частью второй, 355, 359 и 361 Уголовного кодекса Российской Федерации;

3) следователями органов внутренних дел Российской Федерации - по уголовным делам о преступлениях, предусмотренных статьями 111 частями первой - третьей, 113, 114, 117 частями второй и третьей, 122 частями третьей и четвертой, 123 частью третьей, 124, 127.1, 127.2, 150 частями второй и третьей, 151 частями второй и третьей, 158 частями второй - четвертой, **159 частями второй - седьмой, 159.1 частями второй - четвертой, 159.2 частями второй - четвертой, 159.3 частями второй - четвертой, 159.5 частями второй - четвертой, 159.6 частями второй - четвертой**, 160 частями второй - четвертой, 161 частями второй и третьей, 162, 163 частями второй и третьей, 164, 165 частью второй, 166 частями второй - четвертой, 167 частью второй, **171 частью второй, 171.1 частями** первой.1, **второй**, четвертой и шестой, 172, 172.2, 173.1, 173.2, 174, 174.1, 175 частью третьей, 176, 178, 179, 180 частями третьей и четвертой, 181 частью второй, 183, 184, 186, **187**, 191, 191.1 частью третьей, 192, 193, 193.1, 195 - 197, 200.1 частью второй, 200.2, 200.3 частью второй, 201, 202, 205, 206, 207 частью второй, 208 - 210, 212.1, 213 частями второй и третьей, 215.2, 215.3, 217.1, 219 частями второй и третьей, 220 частями второй и третьей, 221 частями второй и третьей, 222 частями второй и третьей, 222.1 частями второй и третьей, 223 частями второй и третьей, 223.1, 225 - 227, 228 частями второй и третьей, **228.1**, 228.4, 229, 229.1, 230 частями второй и третьей, 230.1 частью третьей, 230.2 частью второй, 231 частью второй, 232 частями второй и третьей, 234 частями второй и третьей, 234.1 частями второй и третьей, 235, 236, 240 частями второй и третьей, 241 частями второй и третьей, 243 частью второй, 243.2 частью третьей, 243.3 частью второй, 259, 260 частями второй и третьей, 261 частями третьей и четвертой, 264, 266 частями второй и третьей, 267, 267.1, 268 частями второй и третьей, **272 - 274**, 304, 313 частями второй и третьей, 322.1 частью второй, 325.1 частью второй, 327 частью второй, 327.1 частями второй и четвертой и 330 частью второй Уголовного кодекса Российской Федерации;

"Уголовно-процессуальный кодекс Российской Федерации" от 18.12.2001 N 174-ФЗ (ред. от 03.04.2017)

Статья 151. Подследственность (продолжение)

3. Дознание производится:

1) дознавателями органов внутренних дел Российской Федерации - по всем уголовным делам, указанным в части третьей статьи 150 настоящего Кодекса*, за исключением уголовных дел, указанных в пунктах 3 - 6, 9 настоящей части;

3) дознавателями пограничных органов федеральной службы безопасности - по уголовным делам о преступлениях, предусмотренных статьями 253 и 256 (в части, касающейся незаконной добычи водных животных и растений, обнаруженной пограничными органами федеральной службы безопасности), частями первой и второй статьи 322 и частью первой статьи 323 Уголовного кодекса Российской Федерации;

4) дознавателями органов Федеральной службы судебных приставов - по уголовным делам о преступлениях, предусмотренных статьями 157 и 177, частью первой статьи 294, статьей 297, частью первой статьи 311, статьями 312 и 315 Уголовного кодекса Российской Федерации;

6) дознавателями органов государственного пожарного надзора федеральной противопожарной службы - по уголовным делам о преступлениях, предусмотренных статьей 168, частью первой статьи 219, частями первой и второй статьи 261 Уголовного кодекса Российской Федерации;

7) следователями Следственного комитета Российской Федерации - по уголовным делам о преступлениях, предусмотренных частью третьей статьи 150 настоящего Кодекса, совершенных лицами, указанными в подпунктах "б" и "в" пункта 1 части второй настоящей статьи;

9) дознавателями таможенных органов Российской Федерации - по уголовным делам о преступлениях, предусмотренных статьями 194 частями первой и второй, 200.1 частью первой Уголовного кодекса Российской Федерации.

*Примечание автора: В частности, 159.3 частью первой, 159.6 частью первой, 228 частью первой, 242.

"Уголовно-процессуальный кодекс Российской Федерации" от 18.12.2001 N 174-ФЗ (ред. от 03.04.2017)

Статья 151. Подследственность (продолжение)

4. По уголовным делам о преступлениях, предусмотренных статьями 215.4 частью второй пунктом "б", 275, 276, 283, 283.1 и 284 Уголовного кодекса Российской Федерации, в совершении которых обвиняются лица, указанные в подпункте "в" пункта 1 части второй настоящей статьи, предварительное следствие производится следователями органов федеральной службы безопасности.

5. По уголовным делам о преступлениях, предусмотренных статьями 146, 158 частями третьей и четвертой, 159 частями второй - седьмой, 159.1 частями второй - четвертой, 159.2 частями второй - четвертой, 159.3 частями второй - четвертой, 159.5 частями второй - четвертой, 159.6 частями второй - четвертой, 160 частями второй - четвертой, 161 частями второй и третьей, 162, 171 частью второй, 171.1 частями первой.1, второй, четвертой и шестой, 172, 172.2, 173.1, 173.2, 174, 174.1, 176, 183, 187, 190, 191, 192, 193, 193.1, 194 частями первой и второй, 195 - 197, 200.1 частью первой, 200.2, 201, 202, 205.4, 205.5, 206, 207 частью второй, 208 - 210, 215.4 частью второй пунктом "а", 222 частями второй и третьей, 222.1 частями второй и третьей, 223 частями второй и третьей, 223.1, 226 частями второй - четвертой, 226.1, 228 частями второй и третьей, 228.1, 228.4, 229.1, 234.1 частями второй и третьей, 239, 243 частью второй, 243.2 частью третьей, 243.3 частью второй, 263.1, 272 - 274, 282.1 - 282.3, 284.1, 285, 286, 308, 310, 327 частью второй и 327.1 частями второй и четвертой Уголовного кодекса Российской Федерации, предварительное следствие может производиться также следователями органа, выявившего эти преступления.

6. По уголовным делам о преступлениях, предусмотренных статьями 150, 205.6, 285.1, 285.2, 306 - 310, 311 частью второй, 316 и 320 Уголовного кодекса Российской Федерации, предварительное следствие производится следователями того органа, к чьей подследственности относится преступление, в связи с которым возбуждено соответствующее уголовное дело.

7. При соединении в одном производстве уголовных дел, подследственных разным органам предварительного расследования, подследственность определяется прокурором с соблюдением подследственности, установленной настоящей статьей.

8. Споры о подследственности уголовного дела разрешает прокурор.

Управление «К» МВД России

https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii



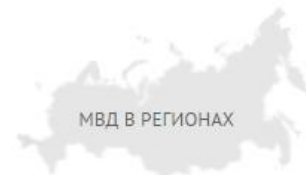
ГОСУСЛУГИ | НАШИ ПРОЕКТЫ | МОБИЛЬНОЕ ПРИЛОЖЕНИЕ

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

СЛУЖИМ РОССИИ, СЛУЖИМ ЗАКОНУ!



ВСЕГДА
НА СВЯЗИ 102



МВД РОССИИ

ДЕЯТЕЛЬНОСТЬ

ДЛЯ ГРАЖДАН

КОНТАКТЫ

ОНЛАЙН-СЕРВИСЫ



[Главная](#) → [МВД России](#) → [Структура Министерства](#) → [Управления](#) → Управление «К» МВД России

Управление «К» МВД России

Начальник Бюро специальных технических мероприятий МВД России генерал-майор
полиции

Мошков Алексей Николаевич



[Новости](#)

[Памятка "Управление «К» предупреждает"](#)

[Управление «К» предупреждает](#)

Новости

Памятка "Управление «К»
предупреждает"

Управление «К» предупреждает

ПРИЕМ ОБРАЩЕНИЙ



ПРАВОВОЕ ИНФОРМИРОВАНИЕ



ГОСУДАРСТВЕННЫЕ УСЛУГИ



ВОПРОСЫ МИГРАЦИИ



Основные направления работы Управления «К» БСТМ МВД России:

1. Борьба с преступлениями в сфере компьютерной информации:

- выявление и пресечение фактов неправомерного доступа к компьютерной информации;
- борьба с изготовлением, распространением и использованием вредоносных программ для ЭВМ;
- противодействие мошенническим действиям с использованием возможностей электронных платежных систем;
- борьба с распространением порнографических материалов с участием несовершеннолетних через сеть Интернет.

2. Пресечение противоправных действий в информационно- телекоммуникационных сетях, включая сеть Интернет:

- выявление и пресечение преступлений, связанных с незаконным использованием ресурсов сетей сотовой и проводной связи;
- противодействие мошенническим действиям, совершаемым с использованием информационно-телекоммуникационных сетей, включая сеть Интернет;
- противодействие и пресечение попыток неправомерного доступа к коммерческим каналам спутникового и кабельного телевидения.

3. Борьба с незаконным оборотом радиоэлектронных и специальных технических средств.

4. Выявление и пресечение фактов нарушения авторских и смежных прав в сфере информационных технологий.

5. Борьба с международными преступлениями в сфере информационных технологий:

- противодействие преступлениям в сфере информационных технологий, носящим международный характер;
- взаимодействие с национальными контактными пунктами зарубежных государств.

6. Международное сотрудничество в области борьбы с преступлениями, совершаемыми с использованием информационных технологий.

БСТМ МВД России активно взаимодействует с правоохранительными органами иностранных государств как на двусторонней, так и многосторонней основе (ООН, «восьмерка», СНГ, СЕ, ЕС, ШОС, АТР и др.).

1990-е

Вопросы компьютерной безопасности были подняты в постсоветской России на официальный уровень в 1992 году с основанием регулярного межведомственного семинара «Криминалистика и компьютерная преступность» для сотрудников МВД и прокуратуры. В дальнейшем предпосылки для создания специализированного отдела МВД создало совершенствование правовой базы: в Уголовном Кодексе России в редакции 1997 года впервые появилась глава, предусматривающая наказание за преступления в сфере компьютерной информации.

Особый отдел по защите IT-безопасности был создан 14 августа 1998 года на базе действовавшего управления «Р», которое отвечало за обеспечение правопорядка в радиоэлектронных и информационных сетях. В 2000 году аналогичные отделы приступили к работе в 81 субъекте Федерации. Изначально подразделение продолжало называться «Управление Р», но в 2001 году после реорганизации было переименовано в «Управление К».

2000—2005

Начиная с 2000 года, число преступлений в Интернете в России ежегодно удваивалось: в 2001 году их было зарегистрировано 3 тыс., в 2002 году — 6 тыс., в 2003 году — 12 тыс. С 2004 года ежегодно регистрируется порядка 15 тыс. В 2004 году 55 % возбуждённых Управлением «К» уголовных дел относились к краже паролей и других сетевых реквизитов, 10,6 % составили компьютерные пиратства, 8 % — распространение порнографии, 4,1 % уголовных дел возбуждено по фактам внедрения в Сеть вредоносных программ. Доля кардинга (мошенничества с пластиковыми картами) в структуре преступлений составила 1,5 %, разглашение конфиденциальной информации — 2,4 %.

В 2000 году по ст. 273 УК РФ (создание и использование вредоносных программ для ЭВМ) было зафиксировано 170 эпизодов, в 2004 году — свыше тысячи. Согласно данным Управления «К», противоправные действия в Интернете совершали преимущественно молодые люди 18—25 лет (58 %), часто имеющие высшее образование, и студенты вузов (в 70 % случаев).

История

2006—2010

В 2008 году сотрудниками Управления «К» рассматривалось 14 тыс. преступлений в Рунете, год спустя их число превысило 17,5 тысяч, из которых оказалось 9489 случаев несанкционированного доступа к компьютерной информации, 2097 фактов распространения вредоносных программ, 1010 кибермошенничеств, 320 преступлений, связанных с детской порнографией.

8 % всех вирусов и другого опасного ПО в европейском сегменте Интернета в 2009 году были выпущены из Рунета (в мировых масштабах наибольшую угрозу компьютерной безопасности представляют интернет-ресурсы Китая, с которых с июня по сентябрь распространён 21 % хакерских разработок).

В сентябре 2010 года, в рамках реформы МВД, Управление «К» (как впоследствии и все прочие подразделения министерства) было выведено за штат ведомства. После этого все сотрудники прошли переаттестацию, штат Управления сократили на одного человека и вернули в структуру МВД в неизменном виде.

2010-е

В январе—мае 2011 года число киберпреступлений увеличилось на 95 % к аналогичному периоду 2010 года. Наиболее частыми, по данным МВД, стали аферы с Интернет-магазинами и торговлей через социальные сети. Не согласилась с такими выводами полиции компания Group-IB, специализирующаяся на компьютерной криминалистике. По её данным, чаще всего в этот период стали происходить мошенничества с интернет-банкингом, нарушения авторских прав и DDoS-атаки. Расхождения с МВД в толковании криминальной статистики эксперты объяснили так: «Каждое подразделение МВД старается заводить такие уголовные дела, по которым просто привлечь виновных к ответственности. Это же не DDoS-атаки, совершаемые высококвалифицированными хакерами — эти уж точно не станут подключаться к выделенной линии, зарегистрированной по месту проживания».

В целом в 2011 году, по данным МВД со ссылкой на международных экспертов, российские кибермошенники заработали \$2 млрд (а всего в мире — \$7 млрд). Самыми распространёнными в Рунете видами преступлений были названы хищения в интернет-банкинге, sms-мошенничества, фишинг, мошенничества в сфере финансовых пирамид, а также внесение сумм по поводу дорогостоящих (но фиктивных) выигрышей.

Почти год спустя после того как в апреле 2011 года хакеры «вырубили» на время доступ к ЖЖ, в том числе к Живому Журналу президента России, Дмитрий Медведев заявил: нужно создать «такие подразделения, которые принципиально новые и ориентированы на выявление и раскрытие очень сложных в технологическом плане преступлений». На это СМИ с иронией заметили, что «такое подразделение» (Управление «К») в России уже есть, правда, оно «не работает».



Алексей Мошков принял участие в открытии VI международного форума «Борьба с мошенничеством в сфере высоких технологий. Antifraud Russia – 2015» **(03 Декабря 2015)**

Данное мероприятие объединяет на одной площадке представителей органов государственной власти, общества и бизнеса. Его основной задачей является выработка совместных подходов к решению проблем безопасности, в первую очередь в банковской и телекоммуникационной отраслях.

На открытии форума выступил начальник Бюро специальных технических мероприятий МВД России генерал-майор полиции Алексей Мошков. Выступая перед участниками, он отметил, что в текущем году силами Управления «К» МВД России была пресечена деятельность десятка преступных групп, занимавшихся хищениями в кредитно-финансовой сфере. Реальный ущерб от их деятельности исчисляется сотнями миллионов рублей, предотвращены хищения на сумму более полутора миллиардов рублей.

В своем выступлении Алексей Мошков сделал акцент на необходимости объединения усилий банковского сообщества в деле противодействия мошенничествам в IT-сфере, а также активизации обмена информацией с созданным на базе Банка России Центром реагирования на компьютерные инциденты в кредитно-финансовой сфере (FinCERT).

«Когда речь заходит о телекоммуникационных технологиях, и в первую очередь о технологиях, применяемых в банковской сфере, необходимо особое внимание уделять вопросам их безопасности. Цена ошибки в этой отрасли – это не только угроза для кошелька граждан, но и угроза российской экономике», - заявил Алексей Мошков.

2016

Сотрудники Управления «К» МВД России пресекли деятельность мошенницы, представлявшей собой сотрудницей органов государственной власти.

21 Октября 11:00

Оперативникам Управления «К» МВД России стало известно о том, что неизвестное лицо, используя телекоммуникационные технологии, осуществляет хищения денежных средств путем злоупотребления доверием. Действуя якобы от имени органов власти, злоумышленник за денежное вознаграждение предлагал своим жертвам трудоустройство на руководящие должности в федеральные министерства и ведомства в обход установленной законодательством процедуры. Стоимость подобного рода услуг исчислялась сотнями тысяч рублей, а оплата осуществлялась дистанционно, путем перечисления денежных средств на заранее подготовленные банковские счета.

В ходе проведения оперативно-розыскных мероприятий было установлено, что к совершению указанных преступлений причастна 57-летняя жительница г.Москвы, скрывающаяся на территории Калужской области.

Злоумышленница была задержана. Возбуждено уголовное дело по ч. 2 ст.159 УК РФ.

Сотрудники МВД России и ФСБ России задержали интернет-хакеров

01 Июня 10:00

«Сотрудниками МВД России совместно с ФСБ России задержаны 50 подозреваемых в совершении многочисленных хищений денежных средств с расчетных счетов юридических лиц, а также с корреспондентских счетов кредитно-финансовых учреждений с использованием вредоносного программного обеспечения», - сообщила официальный представитель МВД России Ирина Волк.

Кроме того, в результате оперативных мероприятий были заблокированы фиктивные платежные поручения на 2 млрд 273 млн рублей

«Следственным департаментом МВД России возбуждено уголовное дело по признакам состава преступления предусмотренного ч. 1 и 2 ст. 210 УК РФ - организация преступного сообщества», - добавила Ирина Волк.

В рамках уголовного дела проведено 86 обысков на территории 15 субъектов Российской Федерации. В ходе обысков получены материалы, подтверждающие причастность подозреваемых к созданию бот-сетей зараженных компьютеров, организации целевых атак на инфраструктуру кредитно-финансовых и государственных учреждений и совершение хищения денежных средств. Изъято большое количество компьютерной техники, электронных носителей, сим-карт, банковских карт, печатей и документов юридических лиц, оформленных на подставных граждан.

Следственно-оперативные мероприятия продолжаются.

В период с середины 2015 года по настоящее время по всей стране зафиксировано 18 целевых атак на автоматизированные рабочие места клиентов банков, ущерб от которых превысил 3 миллиарда рублей. При этом полиция смогла предотвратить возможный ущерб на сумму 2 млрд. 273 млн. рублей.

См. видео от 13.04.2017 г. «Комментарий официального представителя МВД России»

Порядок приема сообщений о происшествии в органах внутренних дел регламентируется следующими основными НПА

1. Федеральный закон от 02.05.2006 N 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»
2. Приказ МВД России от 29.08.2014 N 736 «Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах МВД РФ заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях»

Статья 2. Право граждан на обращение

1. Граждане имеют право обращаться лично, а также направлять индивидуальные и коллективные обращения, включая обращения объединений граждан, в том числе юридических лиц, в государственные органы, органы местного самоуправления и их должностным лицам, в государственные и муниципальные учреждения и иные организации, на которые возложено осуществление публично значимых функций, и их должностным лицам.

...

Статья 4. Основные термины, используемые в настоящем Федеральном законе

Для целей настоящего Федерального закона используются следующие основные термины:

- 1) **обращение гражданина** (далее - обращение) - направленные в государственный орган, орган местного самоуправления или должностному лицу в письменной форме или в форме электронного документа предложение, заявление или жалоба, а также устное обращение гражданина в государственный орган, орган местного самоуправления;
- ...
- 3) **заявление** - просьба гражданина о содействии в реализации его конституционных прав и свобод или конституционных прав и свобод других лиц, либо сообщение о нарушении законов и иных нормативных правовых актов, недостатках в работе государственных органов, органов местного самоуправления и должностных лиц, либо критика деятельности указанных органов и должностных лиц;

...

Статья 11. Порядок рассмотрения отдельных обращений

1. В случае, если в письменном обращении не указаны фамилия гражданина, направившего обращение, или почтовый адрес, по которому должен быть направлен ответ, ответ на обращение не дается. Если в указанном обращении содержатся сведения о подготавливаемом, совершаемом или совершенном противоправном деянии, а также о лице, его подготавливающем, совершающем или совершившем, обращение подлежит направлению в государственный орган в соответствии с его компетенцией.

Приказ МВД России от 29.08.2014 N 736 «Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах МВД РФ заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях»

1. Настоящая Инструкция устанавливает порядок приема, регистрации и разрешения в территориальных органах МВД РФ заявлений и сообщений граждан РФ, иностранных граждан, лиц без гражданства, должностных и иных лиц о преступлениях, об административных правонарушениях, о происшествиях, а также определяет порядок ведомственного контроля за его соблюдением.

2. В территориальных органах МВД России в целях настоящей Инструкции осуществляются:

2.1. Прием, регистрация и разрешение следующих заявлений:

2.1.1. О преступлении - письменное заявление о преступлении, подписанное заявителем; протокол принятия устного заявления о преступлении; заявление о явке с повинной; протокол явки с повинной; рапорт сотрудника органов внутренних дел РФ об обнаружении признаков преступления; материалы, которые направлены ЦБ РФ в соответствии с ФЗ от 10.07.2002 г. N 86-ФЗ "О ЦБ РФ (Банке России)", а также конкурсным управляющим (ликвидатором) финансовой организации для решения вопроса о возбуждении уголовного дела; постановление прокурора о направлении соответствующих материалов в орган предварительного расследования для решения вопроса об уголовном преследовании; поручение прокурора (руководителя следственного органа) о проведении проверки по сообщению о преступлении, распространенному в СМИ; заявление потерпевшего или его законного представителя по уголовному делу частного обвинения; анонимное (без указания фамилии заявителя или почтового либо электронного адреса, по которому должен быть направлен ответ) заявление, содержащее данные о признаках совершенного или готовящегося террористического акта.

2.1.2. Об административном правонарушении - письменное заявление, в котором содержатся сведения, указывающие на наличие события административного правонарушения; рапорт сотрудника органов внутренних дел, в котором содержатся сведения, указывающие на наличие события административного правонарушения.

2.1.3. О происшествии - письменное заявление о событиях, угрожающих личной или общественной безопасности, в том числе о несчастных случаях, дорожно-транспортных происшествиях, авариях, катастрофах, чрезвычайных происшествиях, массовых отравлениях людей, стихийных бедствиях, в отношении которых требуется проведение проверочных действий с целью обнаружения возможных признаков преступления или административного правонарушения.

Приказ МВД России от 29.08.2014 N 736 «Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах МВД РФ заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях»

2.2. Прием, регистрация и разрешение следующих сообщений:

2.2.1. О преступлении - сообщение, изложенное в устной форме*(6), в котором содержится информация об обстоятельствах, указывающих на признаки совершенного или готовящегося преступления; анонимное сообщение, содержащее данные о признаках совершенного или готовящегося террористического акта.

2.2.2. Об административном правонарушении - сообщение, изложенное в устной форме, в котором содержатся сведения, указывающие на наличие события административного правонарушения.

2.2.3. О происшествии - изложенное в устной форме заявление о событиях, указанных в подпункте 2.1.3 настоящего пункта.

3. Прием заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях - получение заявлений и сообщений сотрудником органов внутренних дел, на которого организационно-распорядительными документами руководителя (начальника) территориального органа МВД России либо лица, исполняющего его обязанности, возложены соответствующие полномочия.

4. Регистрация заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях - присвоение каждому принятому (полученному) заявлению (сообщению) очередного порядкового номера Книги учета заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях (приложение N 1 к настоящей Инструкции) и фиксация в ней кратких сведений по существу заявления (сообщения).

5. Разрешение заявлений и сообщений о преступлении, об административном правонарушении, о происшествии - проверка фактов, изложенных в зарегистрированном заявлении (сообщении), уполномоченным должностным лицом территориального органа МВД России и принятие в пределах его компетенции решения в порядке, установленном законодательными и иными нормативными правовыми актами Российской Федерации.

Приказ МВД России от 29.08.2014 N 736 «Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах МВД РФ заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях»

8. Заявления и сообщения о преступлениях, об административных правонарушениях, о происшествиях вне зависимости от места и времени совершения преступления, административного правонарушения либо возникновения происшествия, а также полноты содержащихся в них сведений и формы представления подлежат обязательному приему во всех территориальных органах МВД России.

9. Круглосуточный прием заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях осуществляется оперативным дежурным*(19) дежурной части территориального органа МВД России (управления, отдела, отделения, пункта полиции, линейного отдела, линейного отделения, линейного пункта полиции)*(20).

10. Для приема заявлений о преступлениях, об административных правонарушениях, о происшествиях в электронной форме, направляемых посредством официальных сайтов*(21), применяется программное обеспечение, предусматривающее обязательное заполнение заявителем реквизитов, необходимых для работы с заявлениями о преступлениях, об административных правонарушениях, о происшествиях.

...

14. Вне пределов административных зданий территориальных органов МВД России или в административных зданиях территориальных органов МВД России, в которых дежурные части не предусмотрены, заявления и сообщения о преступлениях, об административных правонарушениях, о происшествиях принимаются уполномоченными сотрудниками органов внутренних дел.

14.1. Сотрудник органов внутренних дел, принявший заявление (сообщение) о преступлении, об административном правонарушении, о происшествии, обязан незамедлительно передать в дежурную часть (по телефону, электронной почте, а также посредством иных доступных видов связи) информацию по существу принятого заявления (сообщения) для регистрации в КУСП. При этом оперативному дежурному дежурной части передается следующая информация:

14.1.1. Дата и время поступления заявления (сообщения).

14.1.2. Фамилия, имя и отчество заявителя.

14.1.3. Адрес места жительства (пребывания), номер телефона заявителя.

14.1.4. Форма фиксации заявления (сообщения) (письменное заявление, протокол явки с повинной и другие).

14.2. На принятом заявлении о преступлении, об административном правонарушении, о происшествии сотрудник органов внутренних дел в обязательном порядке указывает дату и время его получения, свои должность, инициалы, фамилию и заверяет эти сведения своей подписью.

Приказ МВД России от 29.08.2014 N 736 «Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах МВД РФ заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях»

15. В случае если по объективным причинам у сотрудника органов внутренних дел, принявшего заявление (сообщение) о преступлении, об административном правонарушении, о происшествии, отсутствует возможность сообщить в дежурную часть информацию по существу принятого заявления и сообщения, соответствующие сообщение либо подлинник заявления передаются в дежурную часть по прибытии сотрудника в территориальный орган МВД России. При этом указанный сотрудник обязан принять меры к незамедлительной передаче сообщения либо подлинника заявления в дежурную часть.

...

17. При приеме от заявителя письменного заявления о преступлении заявитель предупреждается об уголовной ответственности за заведомо ложный донос в соответствии со статьей 306 Уголовного кодекса Российской Федерации*(24), о чем делается отметка, удостоверяемая подписью заявителя.

...

23. Регистрация в КУСП заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях осуществляется независимо от территории оперативного обслуживания незамедлительно и круглосуточно в дежурных частях.

...

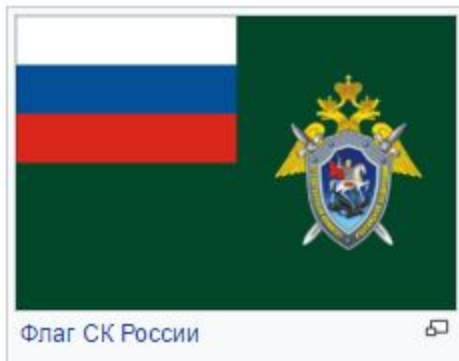
25. КУСП является документом строгой отчетности. КУСП оформляется, регистрируется и брошюруется в соответствии с Правилами делопроизводства в федеральных органах исполнительной власти, утвержденными постановлением Правительства Российской Федерации от 15 июня 2009 г. N 477, а также инструкцией по делопроизводству, согласованной с Росархивом.

26. Обязанности по ведению КУСП и регистрации в ней заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях возлагаются на оперативного дежурного дежурной части.

КУСП заполняется четко и разборчиво. Записи производятся от руки ручкой, без сокращений. Исправления не допускаются. Ошибочные записи зачеркиваются и удостоверяются подписью оперативного дежурного дежурной части. По окончании КУСП передается из дежурной части в подразделение делопроизводства для последующего хранения.

Следственный комитет Российской Федерации

Следственный комитет Российской Федерации (СК России) — федеральный государственный орган в Российской Федерации, осуществляющий полномочия в сфере уголовного судопроизводства и иные полномочия в соответствии с законодательством.



Флаг СК России



Здание Следственного комитета на Бауманской улице

Следственный комитет Российской Федерации
СК России



Страна  Россия
Создана 15 января 2011 года
Юрисдикция Президент Российской Федерации
Средняя численность 23 190
Предшествующая служба Следственный комитет при прокуратуре Российской Федерации
Руководство
Александр Иванович Бастрыкин ^[1]
Сайт
sledcom.ru
[\[http://След.ком.РФ\]](http://След.ком.РФ) sled.com.rf

Следственный комитет РФ

sledcom.ru Следственный Комитет Российской Федерации



СЛЕДСТВЕННЫЙ КОМИТЕТ РОССИЙСКОЙ ФЕДЕРАЦИИ



Бесплатные телефонные линии:

8 (800) 100-12-60
Телефон доверия

8 (800) 200-19-10
"Ребенок в опасности"



БАСТЫРИН АЛЕКСАНДР ИВАНОВИЧ

Председатель Следственного комитета Российской Федерации, генерал юстиции Российской Федерации

[Прямая линия](#) [Блог Председателя СК](#)

СК РОССИИ

ДЕЯТЕЛЬНОСТЬ

НОВОСТИ

ВЗАИМОДЕЙСТВИЕ СО СМИ

РЕЗОНАНСНЫЕ ДЕЛА

ДОКУМЕНТЫ

ПРОТИВОДЕЙСТВИЕ КОРРУПЦИИ



★ ГЛАВНОЕ

🗨️ НОВОСТИ

📷 ФОТО

📺 ВИДЕО

📡 RSS

✉️ ПОДПИСАТЬСЯ НА РАССЫЛКУ



ЧЕТЫРЕМ ЗАДЕРЖАННЫМ В ХОДЕ
НЕСАНКЦИОНИРОВАННОЙ АКЦИИ В
МОСКВЕ ПРЕДЪЯВЛЕНО ОБВИНЕНИЕ

13 Апреля 2017 17:18:04



ВОЗБУЖДЕНО УГОЛОВНОЕ ДЕЛО В
ОТНОШЕНИИ БЫВШЕГО ГЛАВЫ
РЕСПУБЛИКИ МАРИЙ ЭЛ И ЕГО
СОУЧАСТНИКОВ

13 Апреля 2017 12:48:01



НАЧАЛИСЬ СУДЕБНЫЕ СЛУШАНИЯ ПО
УГОЛОВНОМУ ДЕЛУ В ОТНОШЕНИИ
ПОСОБНИКА УБИЙСТВА ЗАМЕСТИТЕЛЯ
ГЛАВЫ АДМИНИСТРАЦИИ
КРАСНОГОРСКОГО МУНИЦИПАЛЬНОГО
РАЙОНА МОСКОВСКОЙ ОБЛАСТИ

13 Апреля 2017 12:11:16



В АРХАНГЕЛЬСКЕ ОРГАНИЗАТОРАМ И
ПЕРСОНАЛУ ИГОРНЫХ КЛУБОВ
ПРЕДЪЯВЛЕНЫ ОБВИНЕНИЯ В
НЕЗАКОННЫХ ОРГАНИЗАЦИИ И
ПРОВЕДЕНИИ АЗАРТНЫХ ИГР

13 Апреля 2017 09:44:10



В САНКТ-ПЕТЕРБУРГЕ ЗАКЛЮЧЕН ПОД
СТРАЖУ ПОДОЗРЕВАЕМЫЙ В
ИЗБИЕНИИ ШКОЛЬНИКА

12 Апреля 2017 17:58:16

ПОДЕЛИТЬСЯ



«ПРЕСТУПЛЕНИЯ ПРОШЛЫХ ЛЕТ»

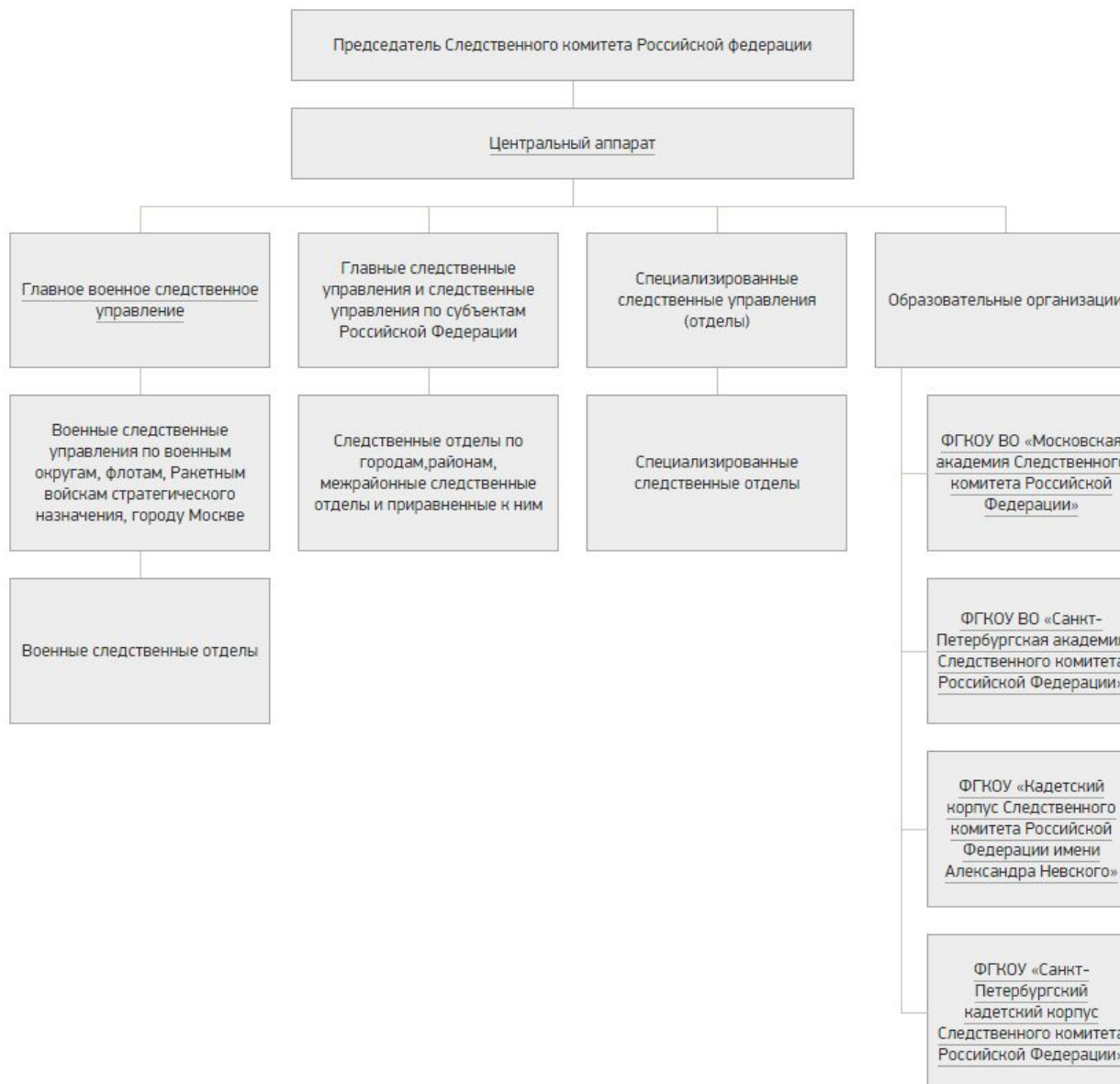
[ВЗАИМОДЕЙСТВИЕ СО СМИ](#) ➔

[МЕРОПРИЯТИЯ](#) ➔

[СМИ О СЛЕДСТВЕННОМ КОМИТЕТЕ](#) ➔

[ИНТЕРВЬЮ](#) ➔

СТРУКТУРА



Порядок приема заявлений о преступлениях

Выписка из Инструкции о порядке приема, регистрации и проверки сообщений о преступлении в следственных органах (следственных подразделениях) системы Следственного комитета Российской Федерации, утвержденной приказом Председателя Следственного комитета Российской Федерации от 03.05.2011 года № 72.

II. Прием сообщений о преступлении

6. Сообщение о преступлении вне зависимости от места и времени совершения преступного деяния, полноты сообщаемых сведений и формы представления, а также подследственности подлежит обязательному принятию (приему) во всех следственных органах СК России.

7. В общедоступных помещениях административных зданий следственных органов СК России на стендах размещаются:

выписки из положений УПК РФ и настоящей Инструкции, регламентирующих порядок приема сообщений о преступлении;

образцы письменного заявления о преступлении, о явке с повинной;

перечень должностных лиц следственного органа СК России, правомочных принимать такие сообщения, а также оформлять протоколы принятия устного заявления о преступлении;

информация о месте, днях и часах личного приема граждан руководителем следственного органа и его заместителем;

сведения о должностных лицах следственных органов СК России, органов прокуратуры и суда (должность, Ф.И.О., адрес органа), которым в соответствии с УПК РФ могут быть обжалованы действия (бездействие) и решения следователя и руководителя следственного органа.

Кроме того, такая информация может быть доведена полностью или частично до сведения граждан через средства массовой информации и размещена на сайте следственного органа СК России.

8. Заявление о преступлении может быть сделано заявителем, прибывшим в следственный орган СК России, в устном или письменном виде.

II. Прием сообщений о преступлении (продолжение)

9. Правомочными осуществлять оформление сообщений о преступлении в соответствии с требованиями УПК РФ являются должностные лица, указанные в подпунктах "а", "б" пункта 2 настоящей Инструкции. Должностные лица, указанные в подпункте "в" пункта 2 настоящей Инструкции, осуществляют оформление сообщений о преступлении при наличии соответствующего поручения руководителя следственного органа СК России.

Круглосуточный прием сообщений о преступлении осуществляется дежурными следователями следственных органов СК России.

Отсутствие дежурного следователя не является основанием для отказа заявителю в приеме от него сообщения о преступлении следователем, руководителем следственного органа либо его заместителем, не привлеченным к дежурству.

Прием руководителем следственного органа СК России или его заместителем граждан с жалобами на отказ подчиненного ему руководителя следственного органа (его заместителя) или следователя в принятии от них сообщения о преступлении осуществляется незамедлительно.

10. Устное сообщение о преступлении на основании части 3 статьи 141 УПК РФ вносится в протокол, который подписывается заявителем и лицом, принявшим заявление. Протокол должен содержать данные о заявителе и документе, удостоверяющем его личность. При этом заявитель предупреждается об уголовной ответственности за заведомо ложный донос в соответствии со статьей 306 Уголовного кодекса Российской Федерации (УК РФ), о чем в протоколе делается отметка, которая удостоверяется подписью заявителя.

11. В случае, когда заявитель не может лично присутствовать при составлении протокола, его заявление на основании части 5 статьи 141 УПК РФ оформляется рапортом об обнаружении признаков преступления в порядке, установленном статьей 143 УПК РФ.

12. Если устное сообщение о преступлении сделано при производстве следственного действия, то оно на основании части 4 статьи 141 УПК РФ вносится в протокол следственного действия. При этом заявитель должен быть предупрежден об уголовной ответственности за заведомо ложный донос в соответствии со статьей 306 УК РФ, о чем в протоколе делается отметка, которая удостоверяется подписью заявителя.

II. Прием сообщений о преступлении (продолжение)

13. Заявителю, обратившемуся в следственный орган с устным заявлением о преступлении, в соответствии с требованиями части 1 статьи 11 УПК РФ должно быть разъяснено право, предусмотренное частью 1 статьи 141 УПК РФ, на подачу письменного заявления о преступлении.

Письменное заявление о преступлении должно в обязательном порядке содержать сведения о заявителе и быть подписано им.

Письменное заявление о преступлении может быть направлено заявителем почтовой связью.

14. При приеме от заявителя заявления о преступлении либо в ходе проверки по заявлению о преступлении заявитель должен быть предупрежден об уголовной ответственности за заведомо ложный донос в соответствии со статьей 306 УК РФ. Факт такого предупреждения подтверждается собственноручной записью заявителя либо отметкой соответствующего должностного лица, которая удостоверяется подписью заявителя.

15. Заявление о явке с повинной может быть сделано в произвольной форме как в письменном, так и в устном виде. Принятое устное заявление о явке с повинной вносится в протокол явки с повинной в порядке, установленном частью 3 статьи 141 УПК РФ.

16. Сообщения о совершенном или готовящемся преступлении могут быть получены из иных источников. Такими источниками могут быть: средства массовой информации <*>, обращения и жалобы граждан; информация, переданная по телефону, телеграфу и иными средствами электронной связи; обращения государственных и иных организаций и др.

<*> Сообщение о преступлении, распространенное в средствах массовой информации, проверяется следователем исключительно по поручению руководителя следственного органа СК России или его заместителя (часть 2 статьи 144 УПК РФ).

При обнаружении в сообщении, полученном из иных источников, информации об обстоятельствах, указывающих на признаки совершенного или готовящегося преступления, правомочным должностным лицом составляется соответствующий рапорт (статья 143 УПК РФ).

Аналогичный рапорт составляется также при отсутствии заявления потерпевшего либо его законного представителя, если преступление совершено в отношении лица, которое в силу зависимого или беспомощного состояния или по иным причинам не может защищать свои права и законные интересы (часть 4 статьи 20 УПК РФ).

17. Должностное лицо, принявшее в соответствии со своими полномочиями лично от заявителя письменное или устное заявление о преступлении, обязано выдать заявителю под роспись в талоне-корешке талон-уведомление о принятии и регистрации заявления о преступлении с указанием времени, даты его принятия, регистрационного номера и своих данных

II. Прием сообщений о преступлении (продолжение)

18. Бланки талонов-уведомлений и талонов-корешков (приложение N 1) являются документами строгой отчетности. Заполненные талоны-корешки сдаются специально уполномоченному должностному лицу следственного органа СК России для отчета и организации их хранения в течение года с момента выдачи талона-уведомления заявителю.

19. Необоснованный отказ правомочного должностного лица принять заявление о преступлении, невнесение в установленном настоящей Инструкцией порядке сообщения о преступлении в книгу регистрации сообщений о преступлении, а также невыдача заявителю талона-уведомления о принятии и регистрации этого заявления недопустимы.

20. Принятые сообщения о преступлении незамедлительно докладываются руководителю следственного органа СК России либо его заместителю.

21. Сообщения, заявления и обращения, которые не содержат сведений об обстоятельствах, указывающих на признаки преступления, не подлежат регистрации в книге регистрации сообщений о преступлении и не требуют проверки в порядке, предусмотренном статьями 144 - 145 УПК РФ.

Поступившие в следственный орган СК России сообщения, заявления, обращения, в которых заявители выражают несогласие с решениями, принятыми судьями, прокурорами, руководителями следственных органов, следователями или иными сотрудниками следственных органов, высказывают предположение о совершении обжалуемыми действиями указанных лиц должностного преступления и ставят в связи с этим вопрос о привлечении этих лиц к уголовной ответственности, также не подлежат регистрации в книге регистрации сообщений о преступлении и не требуют проверки в порядке, предусмотренном статьями 144 - 145 УПК РФ.

В случае поступления указанного сообщения, заявления, обращения от гражданина лично дежурному следователю, следователю, руководителю следственного органа в ходе личного приема оно подлежит обязательному принятию под роспись соответствующего должностного лица, при этом талон-уведомление заявителю не выдается.

Такие сообщения, заявления, обращения регистрируются как входящие документы и рассматриваются в порядке, установленном Федеральным законом от 02.05.2006 N 59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации" или статьей 124 УПК РФ, а также соответствующими организационно-распорядительными документами СК России. Заявители письменно уведомляются руководителем следственного органа СК России или его заместителем о принятом решении с разъяснением права и порядка его обжалования.

Лекция:

Государственная система обеспечения информационной безопасности РФ

Доклад закончен. Прошу задать вопросы