



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Выполняем требования 187-ФЗ

White paper о мониторинге информационной безопасности
и подключении к ГосСОПКА

Версия 2019-10

Оглавление

Что такое ГосСОПКА	2
Внешние угрозы и внутренние проблемы	3
С чем придётся столкнуться	5
Выполнение нормативных требований	5
Сложность технических решений	5
Недостаток ресурсов	6
Процессный хаос	7
Отсутствие поддержки руководства	8
Необходимость лицензии ФСТЭК России	8
Порядок категорирования объектов КИИ	9
Процесс реагирования на инциденты	10
Что и как передавать в ГосСОПКА	11
Способы передачи сведений	11
Какие сведения следует передавать в ГосСОПКА	11
Сведения о категорировании	12
Сведения о защищённости	12
Сведения о нарушениях	12
Сведения о компьютерных инцидентах	13
Сведения об инвентаризации	13
Функции Центра ГосСОПКА	14
Средства ГосСОПКА	14
Состав технических средств	14
Требования к надёжности и доступности	15
Силы ГосСОПКА	15
Первая линия — авангард	15
Вторая линия — исследователи	15
Третья линия — разведчики	16
Как это работает в «Перспективном мониторинге»	17
Сбор событий безопасности	17
ViPNet TIAS	17
LogCollector	18
Фиды угроз	18
Threat Intelligence Platform	18
Система управления инцидентами	19
Центр мониторинга ЗАО «ПМ»	20
Ссылки	20
Авторы	20
Контакты	20
Приложение 1. Нормативная база	21
Федеральные законы	21
Указы Президента Российской Федерации	21
Постановления правительства Российской Федерации	21
Приказы ФСТЭК России	21
Приказы ФСБ России	21
Методические документы ФСБ России	22
Другие документы	22



Что такое ГосСОПКА

ГосСОПКА — это государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Она создаётся для обмена информацией о кибератаках на информационные системы, нарушение или прекращение работы которых крайне негативно скажется на экономике страны или безопасности граждан.

ГосСОПКА выполняет четыре основные задачи:

- прогнозирование ситуации в области информационной безопасности России;
- взаимодействие организаций-владельцев информационных ресурсов (в том числе субъектов критической информационной инфраструктуры);
- контроль защищённости информационных ресурсов от кибератак;
- расследование компьютерных инцидентов.

К ГосСОПКА должны подключиться все субъекты критической информационной инфраструктуры:

- Здравоохранение
- Наука
- Транспорт
- Связь
- Энергетика
- Финансы
- Атомная энергия
- Оборонная промышленность
- Ракетно-космическая промышленность
- Горнодобывающая промышленность
- Metallургия
- Химическая промышленность

Органы государственной власти в некоторых случаях обязаны подключаться к ГосСОПКА, когда, к примеру, имеют отношение к отраслям, отнесённым к КИИ. Либо могут подключаться на добровольной основе, чтобы обеспечить более высокий уровень информационной безопасности и улучшить процедуры выявления и реагирования на инциденты.



Внешние угрозы и внутренние проблемы

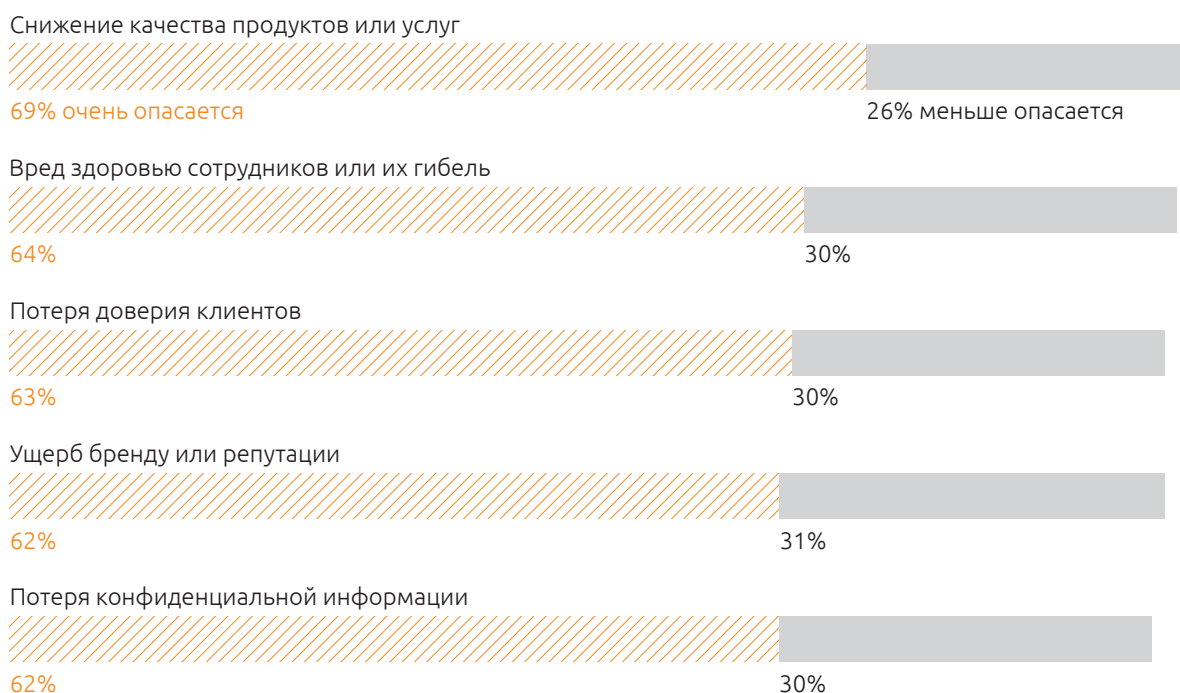
Для атак на критическую информационную инфраструктуру (КИИ) характерны три особенности:

1. Атакующие высоко мотивированы и имеют хорошо отточенные навыки.
2. Атакующие используют неизвестные ранее тактики, техники и процедуры (ТТР).
3. Атакующие присутствуют в инфраструктуре в течение длительного времени и применяют методы сокрытия «следов», из-за чего расследовать такие атаки становится чрезвычайно сложно.

Во время проникновения злоумышленники собирают чувствительную информацию и могут вмешаться в работу технологических процессов. Успешные атаки на КИИ связаны с отсутствием обновлений программного обеспечения промоборудования, ошибками персонала, некорректной настройкой средств защиты и могут потенциально привести к катастрофам.

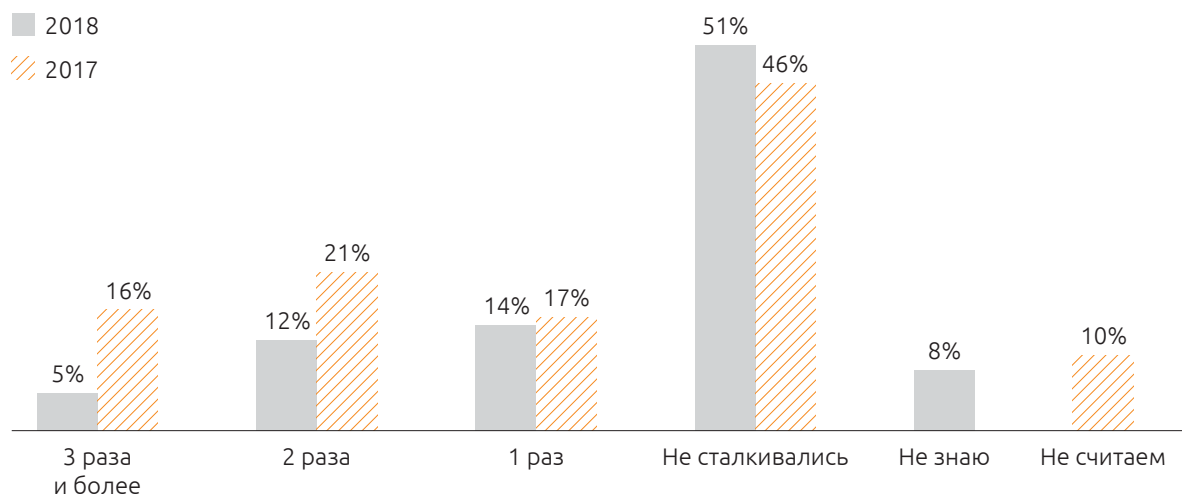
В проведённом в 2018 году исследовании компании Pierre Audoin Consultants (PAC), входящей в СХР Group, авторы опросили 320 руководителей с правом принятия решений по вопросам безопасности АСУТП из компаний по всему миру. Главным риском эти специалисты видят снижение качества сервисов, потерю доверия клиентов и ущерб здоровью или гибель сотрудников в результате киберинцидентов.

Каких последствий опасается ваша компания в случае нарушения кибербезопасности АСУТП?



Треть опрошенных в этом же исследовании специалистов уже сталкивались с какими-либо инцидентами информационной безопасности за последний год. Но даже это не является главной проблемой — инциденты происходили и будут происходить. Почти 20% компаний либо не считают количество инцидентов, либо вообще не знают, была ли атакована их инфраструктура!

Сколько раз за последние 12 месяцев ваша организация сталкивалась с какими-либо инцидентами кибербезопасности, касающимися АСУТП и/или промышленных сетей?



В исследовании, проведённом компанией ИнфоТеКС в рамках цикла региональных конференций «Будни информационной безопасности» в 2017–2018 годах, респонденты из организаций субъектов КИИ указывали на недостаточное оснащение своих систем защиты информации именно средствами обнаружения и предотвращения компьютерных атак.

BSI в своей публикации «Industrial Control System Security — Top 10 Threats and Countermeasures» указывают на TOP-10 угроз индустриальным системам:

1. Социальная инженерия и фишинг.
2. Проникновение вредоносного ПО со съёмных носителей.
3. Проникновение вредоносного ПО через Интернет или интранет.
4. Проникновение через удалённый доступ.
5. Человеческие ошибки и саботаж.
6. Доступность АСУТП из Интернета.
7. Технические неисправности и форс-мажор.
8. Компрометация облачных компонентов.
9. (D)DoS-атаки.
10. Компрометация мобильных устройств в промышленном окружении.

С чем придётся столкнуться

Выполнение нормативных требований

В этом вопросе на деятельность ИБ-персонала влияют два главных фактора.

Первый — достаточно серьёзная ответственность за невыполнение требований. Согласно статье 274.1 Уголовного кодекса наказываются создание вредоносного ПО для неправомерного воздействия на КИИ; неправомерный доступ к охраняемой информации, содержащейся в КИИ; нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой информации, если оно повлекло причинение вреда КИИ.

Если эти действия повлекли тяжкие последствия, то виновный наказывается лишением свободы на срок от пяти до десяти лет.

Второй фактор — большое количество нормативно-правовых документов, регулирующих деятельность субъектов ГосСОПКА, список которых по состоянию на март 2019 года приведён в Приложении 1.

ФСТЭК России и ФСБ России выполняют основные функции контроля в области обеспечения безопасности объектов КИИ. Они же занимаются нормативно-правовым регулированием. ФСТЭК России ведёт реестр значимых объектов КИИ, формирует и контролирует реализацию требований по обеспечению их безопасности. ФСБ России регулирует и координирует деятельность субъектов КИИ, собирает информацию об инцидентах и разрабатывает требования к средствам обнаружения, предотвращения и ликвидации компьютерных атак. Не надо забывать и про надзорные мероприятия, которые регуляторы начнут проводить, когда закончится время, отведенное субъектам КИИ на выполнение требований.

Сложность технических решений

Персонал, отвечающий за информационную безопасность объектов критической информационной инфраструктуры, столкнётся с двумя вызовами.

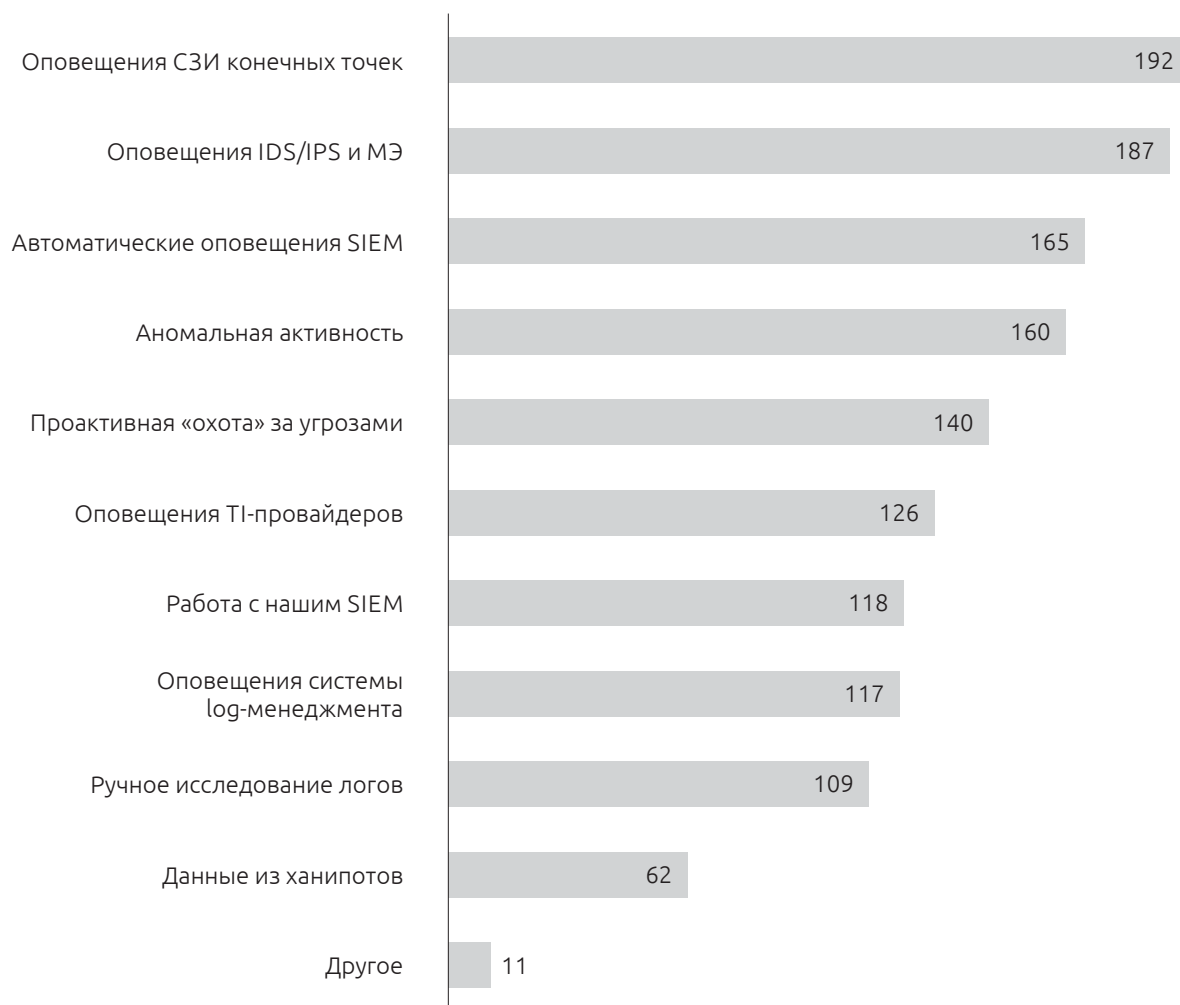
Первый — это целый «зоопарк» технических решений с очень условной на практике совместимостью. Средства обнаружения на сети от одного вендора, на конечных точках — от другого, система управления инцидентами — от третьего. А производители SIEM-решений утверждают, что только благодаря их продукту можно интегрировать весь этот набор в «эффективное средство обнаружение инцидентов информационной безопасности».

Второй — обратная ситуация, когда СОБИ создаётся на базе решений одного вендора. Клиент получает прекрасную совместимость, но за большие деньги и с увеличением зависимости от одного поставщика.



Вместе с тем нельзя отдавать предпочтение только какому-то одному способу обнаружения компьютерных инцидентов. Об этом говорят и лучшие практики. В 2018 году SANS Institute опубликовал исследование «The Definition of SOC-cess? SANS2018 Security Operations Center Survey». Согласно этому исследованию процесс реагирования на инциденты запускают, в основном, оповещения средств защиты конечных точек, сетевых сенсоров и SIEM-решений.

Триггеры реагирования (251 ответ)



Недостаток ресурсов

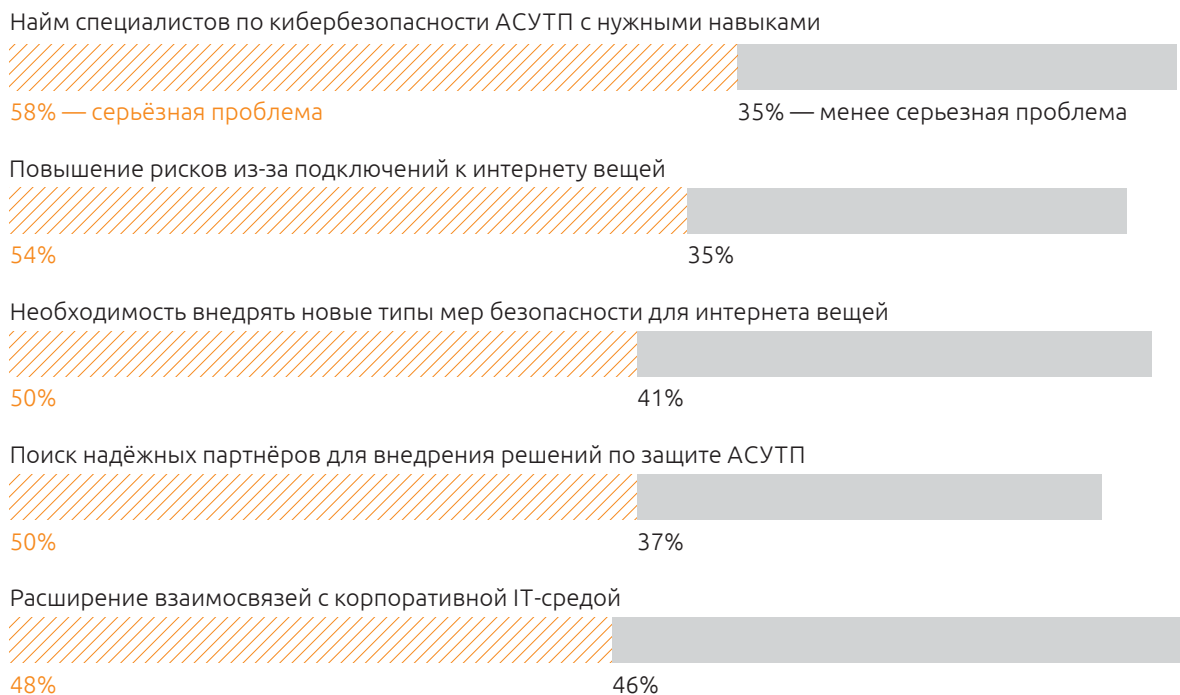
«Нет денег» и «Нет людей» — основные проблемы, на которые указали сотрудники служб ИБ в регионах, посетившие конференции «Будни информационной безопасности» в различных городах России в 2017 и 2018 годах.

С ними согласны и респонденты исследования PAC (СХР Group). Если организация планирует развивать направление защиты промышленных систем и критически важных

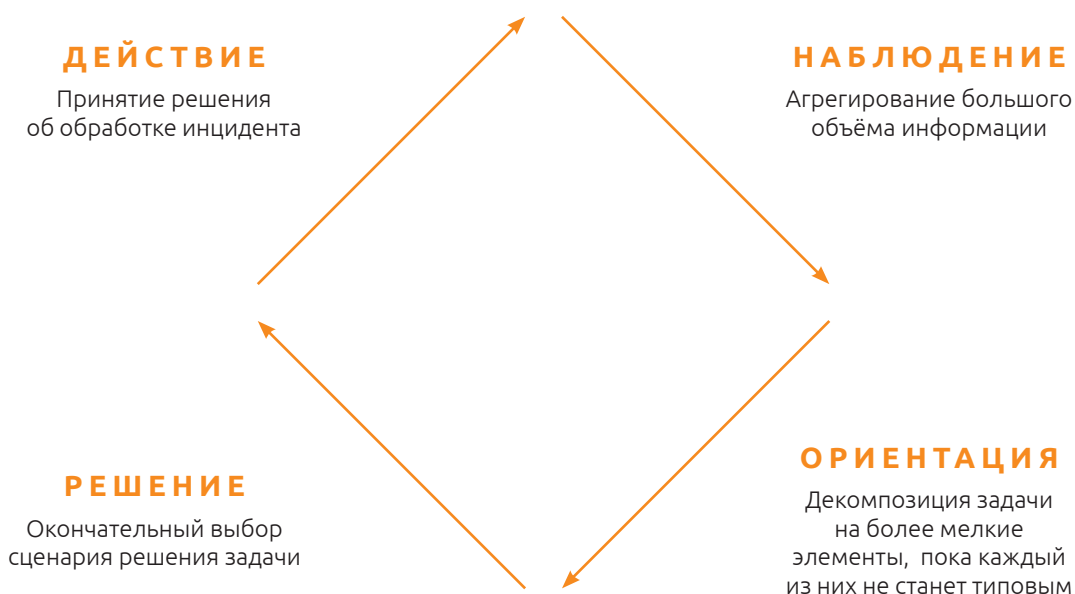


объектов, она наверняка столкнётся с проблемой найма компетентных сотрудников. Дело тут и в общем дефиците ИБ-кадров, и в относительной «молодости» специализации «ИБ для промышленности».

Степень проблематичности факторов, влияющих на безопасность АСУТП



Процессный хаос



Цикл Бойда как верхнеуровневая модель управления инцидентами



Поскольку процесс реагирования на инциденты и противостояния злоумышленникам основан на многократном повторении и последовательном и постоянном совершенствовании, каждый этап цикла должен быть формализован и описан. Иначе невозможно повторять определённые действия с хотя бы такой же эффективностью.

Время + люди + деньги + условия SLA



Время реагирования + количество инцидентов +
+ «счастье пользователей» + compliance

В ситуации, когда только какой-нибудь один сотрудник обладает необходимыми знаниями и навыками по этапу цикла, выход его из строя может стать проблемой всей организации и затормозить процесс. Когда есть фреймворк, ситуации гораздо сложнее выйти из-под контроля.

Отсутствие поддержки руководства

К сожалению, позиция руководства субъектов КИИ по вопросу подключения к ГосСОПКА пока звучит как «Ещё одна „обязаловка“, за которую и посадить могут». Однако, постоянный мониторинг и своевременная подготовка помогут избежать самых негативных последствий кибератак на объекты КИИ, о которых говорилось в начале: снижение качества продукции и сервисов, вред здоровью людей, потеря конфиденциальной информации.

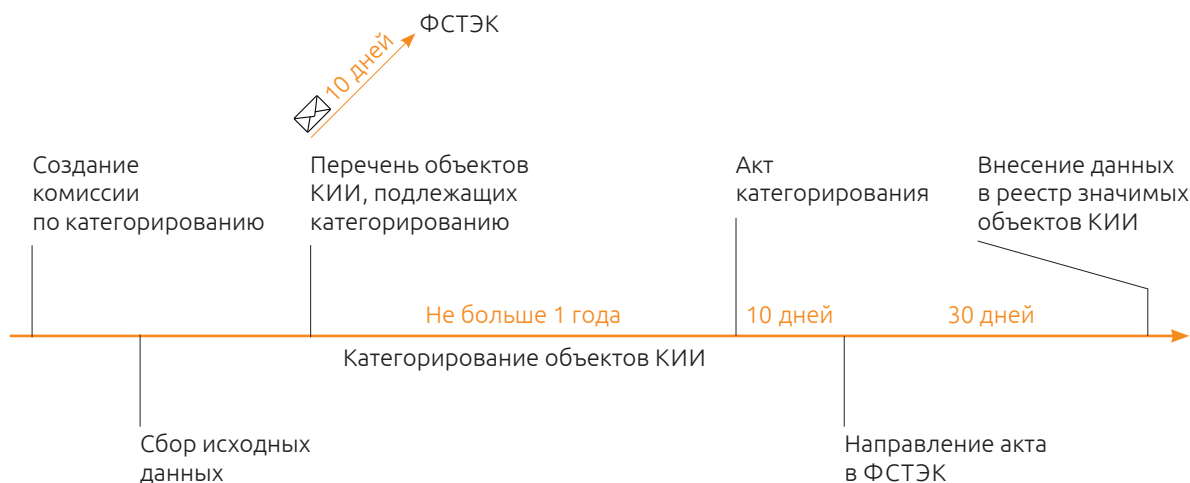
Необходимость лицензии ФСТЭК России

Позиция регулятора в этом вопросе однозначна: если организация хочет оказывать услуги по мониторингу информационной безопасности и подключению к ГосСОПКА для сторонних заказчиков, в её лицензии на техническую защиту конфиденциальной информации должен быть соответствующий пункт. Требования к наличию такой лицензии также предъявляются ФСБ России к организациям, которые решили стать центром ГосСОПКА.

Если эти функции выполняются только для себя, то лицензия не нужна. Однако, это не отменяет необходимости соблюдения всех остальных требований.



Порядок категорирования объектов КИИ



Руководитель организации создаёт постоянно действующую комиссию по категорированию. Она выявляет критичные процессы субъекта КИИ:

- управленческие;
- технологические;
- производственные;
- другие.

Комиссия определяет объекты КИИ, связанные с этими процессами. Перечень объектов в течение десяти рабочих дней после утверждения направляется во ФСТЭК России. ФСТЭК России согласует полученный перечень в течение пяти дней.

Объекту КИИ присваивается одна из трёх категорий значимости или устанавливается отсутствие необходимости присвоения категории. При выборе категории объект оценивается по показателям критериев значимости. Всего существует пять групп показателей, включающих от одной до пяти подгрупп. Итоговая оценка ставится по максимальному значению из всех групп и подгрупп. Подробное описание категорий приведено в Постановлении Правительства № 127.

По результатам работы члены комиссии составляют Акт категорирования объекта КИИ, который утверждается руководителем субъекта КИИ.

Максимальный срок категорирования не должен превышать одного года со дня утверждения субъектом КИИ перечня объектов.

Сведения о результатах категорирования направляются в ФСТЭК России в течение десяти рабочих дней в печатном и электронном виде. Реестр значимых объектов формируется и ведётся ФСТЭК России на основании данных, предоставляемых субъектами КИИ.

Субъекты КИИ должны направлять сведения об изменении категории значимости в ФСТЭК России. Такое изменение может произойти, если:

- ФСТЭК России приняла такое решение по результатам проверки, выполненной в рамках государственного контроля в области обеспечения безопасности значимых объектов КИИ.
- Объект перестал соответствовать критериям значимости.
- Субъект КИИ был реорганизован, ликвидирован или произошли изменения в его организационно-правовой форме.

Субъект КИИ не реже чем один раз в пять лет пересматривает категорию значимости и информирует ФСТЭК России об изменениях.

Если комиссия по категорированию определит отсутствие категории значимости у объекта КИИ, результаты категорирования всё равно должны быть представлены во ФСТЭК России. Служба проверит представленные документы и направит замечания, которые должен учесть субъект, если это будет необходимо.

Процесс реагирования на инциденты



Что и как передавать в ГосСОПКА

Способы передачи сведений

Существует два способа передачи необходимых сведений в НКЦКИ:

1. С использованием технической инфраструктуры НКЦКИ.
2. Посредством электронной, факсимильной, почтовой и телефонной связи.

В первом случае субъект КИИ подключается к инфраструктуре самостоятельно или через Центры ГосСОПКА (корпоративные, ведомственные и т.д.).



Независимо от выбранного способа подключения, ответственные сотрудники субъекта КИИ обязаны сообщить о компьютерном инциденте в течение 3-х часов для значимых объектов КИИ и в течение 24-х часов для остальных объектов КИИ с момента его обнаружения.

В настоящее время подключиться к технической инфраструктуре НКЦКИ возможно, только используя продукты ViPNet, сертифицированные по классу защиты КСЗ.

Какие сведения следует передавать в ГосСОПКА

Приказ ФСБ России № 367 определяет состав и порядок предоставляемой в ГосСОПКА информации. Это сведения о:

- категорировании объекта;
- защищённости информационных ресурсов, доступных из Интернета;
- нарушении требований по обеспечению безопасности;
- компьютерных инцидентах и атаках, связанных с функционированием объекта;



- самостоятельно обнаруженных индикаторах компрометации информационных ресурсов;
- составе информационных ресурсов (инвентаризация).

Сведения о категорировании

Передаются любые сведения о присвоении или изменении категорий значимости.

Подробности в разделе «Порядок категорирования объектов КИИ».

Сведения о защищённости

В НКЦКИ передаются сведения о регулярно проводимых тестированиях на проникновение и результаты работы автоматизированных средств оценки защищённости информационных ресурсов.

Тип контроля	Периодичность контроля, не реже
Выявление уязвимостей сетевых служб, доступных для сетевого взаимодействия	Раз в месяц
Выявление уязвимостей ПО (системное сканирование, исследование с использованием привилегированных учетных записей и (или) программных агентов)	Раз в месяц
Пентест со стороны Интернета	Раз в год
Пентест со стороны контролируемых ресурсов	Раз в год
Тестирование устойчивости к атакам типа «отказ в обслуживании»	Раз в год
Контроль устранения ранее выявленных уязвимостей и недостатков	Раз в квартал
Контроль выполнения требований к безопасности информации	Раз в квартал
Анализ настройки программного и аппаратного обеспечения информационных систем, а также средств защиты информации	Раз в квартал
Анализ проектной, конструкторской и эксплуатационной документации информационных систем	Перед вводом информационного ресурса в эксплуатацию и при каждом существенном изменении состава программных или аппаратных средств

Сведения о нарушениях

Функции государственного контроля в области безопасности значимых объектов КИИ возложены на ФСТЭК России. Если сотрудники службы в рамках плановых и внеплановых проверок обнаружат какие-либо нарушения или несоответствия требованиям, такая информация также должна быть передана в НКЦКИ.



Сведения о компьютерных инцидентах

В НКЦИ передаётся информация о компьютерных инцидентах, связанных с функционированием объектов КИИ:

- дата, время, место нахождения или географическое местоположение объекта КИИ, на котором произошёл компьютерный инцидент;
- наличие причинно-следственной связи между компьютерным инцидентом и компьютерной атакой;
- связь с другими компьютерными инцидентами (при наличии);
- состав технических параметров компьютерного инцидента;
- последствия компьютерного инцидента.

The screenshot displays the NKCI interface for an incident titled "Потенциальная попытка проведения атаки SQL-injection на узел контролируемой инфраструктуры". The incident is categorized as "Эксплуатация уязвимостей" with a "Высокий" (High) severity level. It was detected on 17.10.2018 at 09:41. The interface includes a description, a list of recommended actions (such as blocking the active asset and auditing for vulnerabilities), and a detailed log of events. The log table below shows the following data:

Дата	Порт получателя	IP получателя	Порт отправителя	IP отправителя	Сектор	Правило
17.10.2018 08:46	80	192.168.0.2	56735	91.59.66.41	10.0.24.201	ET WEB_S
17.10.2018 08:46	80	192.168.0.2	56736	91.59.66.41	10.0.24.201	ET WEB_S
17.10.2018 08:46	80	192.168.0.2	56737	91.59.66.41	10.0.24.201	ET WEB_S
17.10.2018 08:46	80	192.168.0.2	56738	91.59.66.41	10.0.24.201	ET WEB_S
17.10.2018 08:46	80	192.168.0.2	56739	91.59.66.41	10.0.24.201	ET WEB_S
17.10.2018 08:46	80	192.168.0.2	56740	91.59.66.41	10.0.24.201	ET WEB_S
17.10.2018 08:46	80	192.168.0.2	56741	91.59.66.41	10.0.24.201	ET WEB_S
17.10.2018 08:46	80	192.168.0.2	56742	91.59.66.41	10.0.24.201	ET WEB_S
17.10.2018 08:46	80	192.168.0.2	56743	91.59.66.41	10.0.24.201	ET WEB_S
17.10.2018 08:46	80	192.168.0.2	56744	91.59.66.41	10.0.24.201	ET WEB_S

Карточка инцидента

Сведения об инвентаризации

Данные о подконтрольных информационных ресурсах собираются при опросе сотрудников и при помощи автоматизированных средств и актуализируются не реже одного раза в квартал.

В состав этих сведений включаются:

- Ф.И.О., должности и контактные данные лиц, ответственных за функционирование информационного ресурса;
- доменные имена и сетевые адреса средств вычислительной техники, телекоммуникационного оборудования, виртуальных машин и т.п.;
- доменные имена и сетевые адреса ресурсов, доступных из Интернета, и сведения о протоколах, по которым разрешён доступ;
- схемы сегментации и топологии ЛВС, правила маршрутизации и коммутации, настройки средств межсетевое экранирования;
- перечень прикладного и системного ПО, установленного на каждом средстве вычислительной техники.



Функции Центра ГосСОПКА

Центр ГосСОПКА должен выполнять следующие функции в отношении контролируемых информационных ресурсов:

- взаимодействие с НКЦКИ;
- подготовка методологической базы;
- эксплуатация средств защиты;
- инвентаризация;
- анализ уязвимостей;
- анализ угроз;
- повышение квалификации персонала;
- приём сообщений о возможных инцидентах от персонала и пользователей;
- обнаружение компьютерных атак;
- анализ данных о событиях безопасности;
- регистрация инцидентов;
- реагирование на инциденты и ликвидация их последствий;
- установление причин инцидентов;
- анализ результатов устранения последствий инцидентов.

Средства ГосСОПКА

Состав технических средств

Средства ГосСОПКА — это техническое обеспечение процессов обнаружения, предупреждения и ликвидации последствий компьютерных атак. Для этих целей могут использоваться:

Средства обнаружения:

- сетевые средства обнаружения вторжений;
- хостовые средства обнаружения вторжений;
- система анализа событий ИБ и выявления инцидентов;
- средства выявления и устранения DDoS-атак;
- система сбора, анализа и корреляции событий из разнородных источников;

Средства ликвидации последствий:

- система регистрации и обработки инцидентов;

Средства обмена и криптографические средства защиты информации:

- СКЗИ для защищённого обмена информацией с другими центрами ГосСОПКА.

Вспомогательные средства технические средства:

- средства межсетевого экранирования;
- средства антивирусной защиты и «песочницы»;
- средства анализа защищённости и управления уязвимостями;



Субъекты КИИ вправе самостоятельно определять состав технических средств, принимая во внимание Приказы ФСТЭК №№ 31, 235, 239.

Пример состава технических средств приведён в разделе «Как это работает в «Перспективном мониторинге».

Требования к надёжности и доступности

Центры, оказывающие услуги по подключению субъектов КИИ к ГосСОПКА, как правило, обеспечивают доступность сервисов на уровне не менее 98% времени. Это достигается благодаря резервированию по питанию, связи и оборудованию. Часто оборудование дублируется на двух независимых площадках.

Силы ГосСОПКА

Центры ГосСОПКА должны проектироваться так, чтобы иметь возможность выполнять возложенные на них функции. Для решения этих задач регулятор предлагает использовать структуру, состоящую из первой, второй и третьей линий специалистов. К силам также относятся сотрудники субъекта, обеспечивающие безопасность значимых объектов КИИ.

Первая линия — авангард

Специалисты первой линии всегда первыми получают информацию о подозрении на инцидент информационной безопасности, и именно на них ложится основная нагрузка, связанная с выявлением и регистрацией инцидентов.

Эта группа — работает постоянно, когда Центр ГосСОПКА оказывает услуги.

Специалисты первой линии выполняют следующие функции:

- принимают сообщения от служб ИБ и пользователей информационных ресурсов об инцидентах (подозрениях на инцидент);
- анализируют события ИБ, выявляют и проводят первичную обработку инцидентов, при необходимости передают инциденты на вторую и третью линии поддержки.

Вторая линия — исследователи

Основная задача сотрудников второй линии центра — расследование инцидентов информационной безопасности и выявление уязвимостей в контролируемых информационных ресурсах. Когда расследуются инциденты, именно их задача — понять, что именно произошло, определить вектор атаки, выявить, какие ресурсы были атакованы, и определить ответственных за инцидент. Кроме этого, они моделируют действия потенциального злоумышленника, проводя регулярные пентесты.

Функции второй линии:

- расследуют инциденты, устанавливают причины;



- находят уязвимости;
- сканируют контролируруемую сеть с целью выявления уязвимых и неизвестных хостов;
- проводят пентесты;
- координируют действия групп реагирования, предоставляют рекомендации по реагированию и обработке инцидентов;
- обеспечивают взаимодействие с НКЦКИ;
- готовят периодические отчёты по инцидентам информационной безопасности.

Третья линия — разведчики

Сотрудники третьей линии занимаются разведкой кибеугроз — Threat Intelligence. Они разрабатывают способы обнаружения ранее неизвестных атак и анализируют текущие и потенциальные угрозы безопасности информации. Они стараются определить, к каким атакам стоит готовиться субъектам критической информационной инфраструктуры.

Функции третьей линии:

- проводят детальный анализ инцидентов, готовят доказательную базу;
- проводят реверс-инжиниринг выявленного вредоносного программного обеспечения, определяют логику его работы;
- анализируют дампы сетевого трафика с целью выявления вредоносной активности;
- предоставляют рекомендации по повышению уровня защищённости;
- создают сигнатуры для сетевых и хостовых IDS, в том числе на основе сведений о выявленных инцидентах;
- создают правила корреляции для средств выявления инцидентов на основе анализа событий ИБ;
- собирают и анализируют сведения о текущих угрозах ИБ;
- администрируют системы регистрации и управления инцидентами.

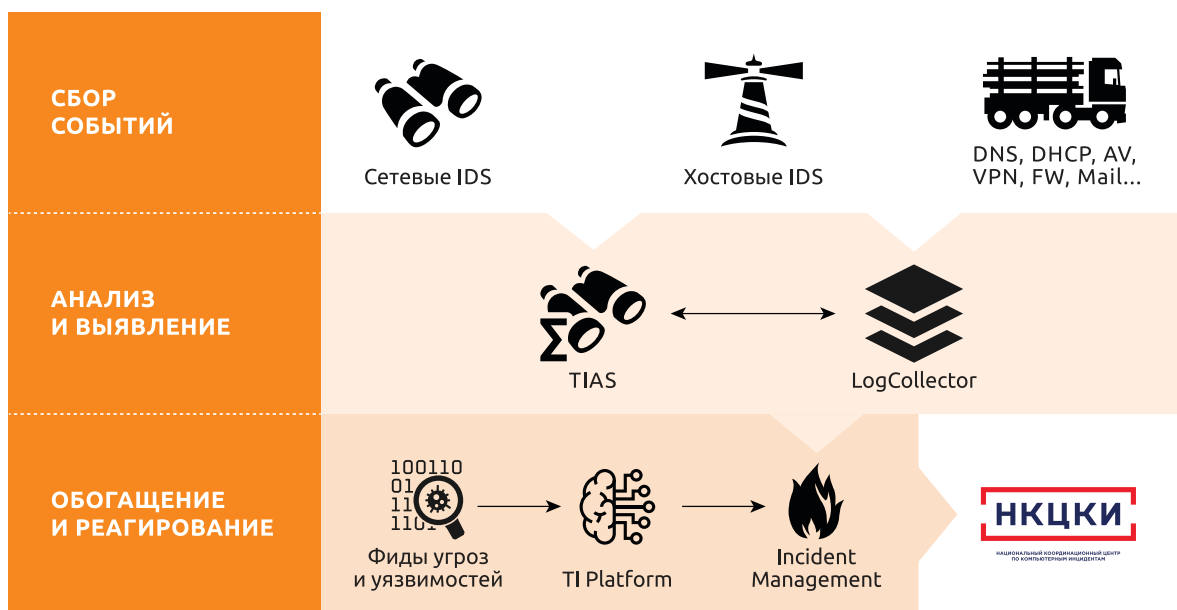
Функции всех трёх линий Центра ГосСОПКА можно свести в одну таблицу.

Авангард	Исследователи	Разведчики
Взаимодействие с пользователями	Расследование инцидентов и помощь в реагировании	Подготовка и улучшение нормативной базы
Анализ событий Выявление инцидентов	Координация работы группы реагирования	Разработка сигнатур и правил корреляции
Регистрация инцидентов	Анализ уязвимостей Анализ защищённости Пентесты	Углублённый анализ инцидентов Сбор доказательств

Кроме трёх перечисленных линий важную роль играют сотрудники группы технического сопровождения, которые отвечают за обеспечение доступности сервисов, корректность функционирования, решение сетевых проблем, работу ИТ-инфраструктуры в целом.



Как это работает в «Перспективном мониторинге»



Сбор событий безопасности

Журналы событий информационной безопасности различных средств защиты и сетевого оборудования отправляются в ViPNet TIAS (ИнфоТеКС) или в собственную разработку «Перспективного мониторинга» — решение LogCollector.

ViPNet TIAS

ViPNet TIAS (Threat Intelligence Analytics System) — программно-аппаратный комплекс, предназначенный для автоматического выявления инцидентов на основе анализа событий информационной безопасности.

ViPNet TIAS в автоматическом режиме анализирует весь поток входящих событий от сенсоров, находит взаимосвязи между ними и выявляет действительно значимые угрозы, являющиеся инцидентами информационной безопасности.

Автоматическое выявление инцидентов информационной безопасности в ViPNet TIAS строится на основе комбинирования двух методов:

- Сигнатурный метод анализа, основанный на использовании метаправил выявления инцидентов.
- Математическая модель принятия решений, разработанная на основе статистического анализа угроз с использованием методов машинного обучения.

База метаправил и математическая модель принятия решений разрабатывается и обновляется экспертами «Перспективного мониторинга».

LogCollector

LogCollector — система обработки данных, предназначенная для сбора и анализа событий от разнородных источников в информационной сети заказчика.

LogCollector состоит из следующих компонентов:

- **Парсер логов** обрабатывает логи в режиме реального времени, динамически объединяет данные из различных источников, фильтрует и нормализует их.
- **Агент сбора логов** позволяет собирать логи с узлов, которые не отправляют их самостоятельно. Собранные события передаются в парсер логов.
- **Нереляционная база данных** индексирует и хранит все события от различных источников.
- **Система визуализации данных** строит произвольные дашборды и предоставляет различные разрезы данных.
- **Система анализа событий** выявляет всплески, аномалии, появления новых значений.
- **Система очередей** контролирует потоки данных, гарантируя доставку.
- **Система безопасности** реализует авторизацию и аутентификацию пользователей и разграничивает права доступа.

Фиды угроз

На март 2019 года Центр мониторинга получает данные из 18 различных источников: опасные IP-адреса, домены, образцы и хеши образцов вредоносного программного обеспечения, различные индикаторы компрометации.

Threat Intelligence Platform

Threat Intelligence Platform собственной разработки «Перспективного мониторинга» решает три задачи:

1. Сбор данных из различных источников.
2. Обработка, интерпретация, унификация и хранение данных об угрозах.
3. Применение TI для выявления инцидентов.

СБОР

- Фиды угроз
- Образцы трафика
- Образцы ВПО
- honeypots
- Ручное добавление

Все эти данные «проигрываются» различными обработчиками

ОБРАБОТКА

- Песочница
- Парсеры
- Автотаггеры
- IDS/Snort-обработчики
- Анализатор http-сессий
- DGA-модели
- MO-модели
- VirusTotal
- Поиск «почти одинаковых» файлов (ssdeep-model)

Каждый обработчик (или их «команда») выносят вердикт об опасности образца

ПРИМЕНЕНИЕ

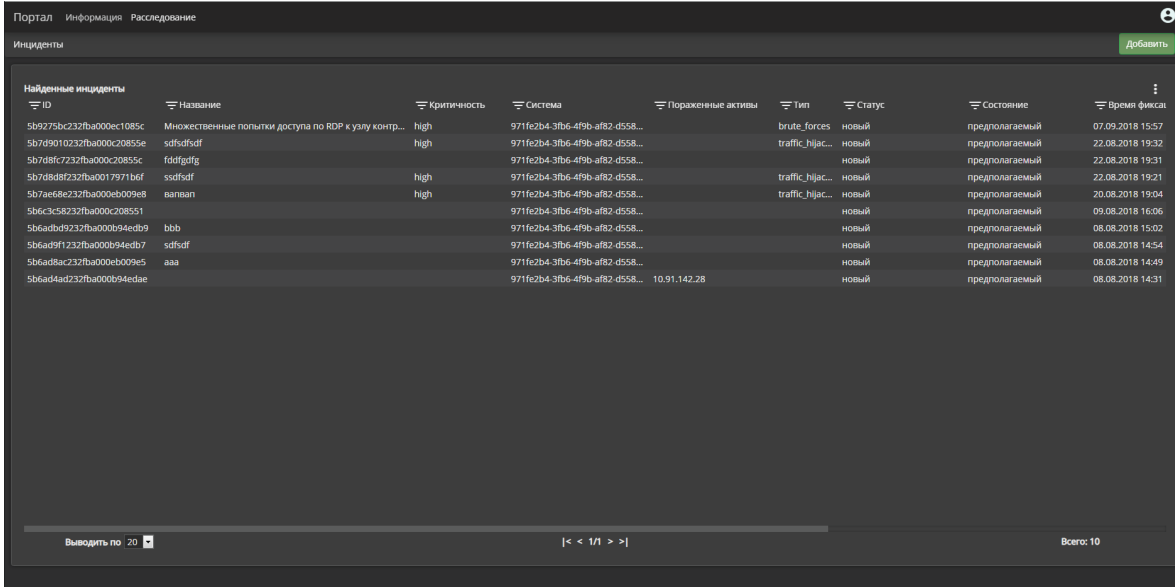
- Данные для написания сигнатур IDS
- Данные для написания правил корреляции LogCollector
- Ретроспективный анализ событий
- Обогащение карточки инцидента в системе Incident Management

Вердикты обработчиков помогают выявлять инциденты ИБ



Благодаря API TI Platform интегрируется с системой управления инцидентами, TIAS, SIEM-системами и помогает группам мониторинга, выдавая интегральную оценку зловредности для ip-адресов, доменов и подозрительных файлов.

Система управления инцидентами



Портал Информация Расследование

Инциденты Добавить

Найденные инциденты	ID	Название	Критичность	Система	Пораженные активы	Тип	Статус	Состояние	Время фикса:
	5b9275bc232fba000ec1085c	Множественные попытки доступа по RDP к узлу контр...	high	971fe2b4-3fb6-4f9b-af82-d558...		brute_forces	новый	предполагаемый	07.09.2018 15:57
	5b7d9010232fba000c20855e	sdfsdf	high	971fe2b4-3fb6-4f9b-af82-d558...		traffic_hjac...	новый	предполагаемый	22.08.2018 19:32
	5b7d8f7232fba000c20855c	fdfdgdfg		971fe2b4-3fb6-4f9b-af82-d558...			новый	предполагаемый	22.08.2018 19:31
	5b7d8d8f232fba0017971b6f	ssdfsdf	high	971fe2b4-3fb6-4f9b-af82-d558...		traffic_hjac...	новый	предполагаемый	22.08.2018 19:21
	5b7ae68e232fba000eb009e8	baiban	high	971fe2b4-3fb6-4f9b-af82-d558...		traffic_hjac...	новый	предполагаемый	20.08.2018 19:04
	5b6c3c58232fba000c208551			971fe2b4-3fb6-4f9b-af82-d558...			новый	предполагаемый	09.08.2018 16:06
	5b6adb9232fba000b94edb9	bbb		971fe2b4-3fb6-4f9b-af82-d558...			новый	предполагаемый	08.08.2018 15:02
	5b6ad9f1232fba000b94edb7	sdfsdf		971fe2b4-3fb6-4f9b-af82-d558...			новый	предполагаемый	08.08.2018 14:54
	5b6ad8ac232fba000eb009e5	aaa		971fe2b4-3fb6-4f9b-af82-d558...			новый	предполагаемый	08.08.2018 14:49
	5b6ad4ad232fba000b94edae			971fe2b4-3fb6-4f9b-af82-d558... 10.91.142.28			новый	предполагаемый	08.08.2018 14:31

Выводить по 20 | < < 1/1 > > | Всего: 10

Управление инцидентами — один из важнейших процессов управления информационной безопасностью. Организациям важно правильно и своевременно отслеживать обработку инцидентов: идентифицировать, классифицировать, информировать, сдерживать, расследовать и устранять последствия.

В Системе управления инцидентами главной сущностью является карточка инцидента, в которой собирается вся связанная с инцидентом информация и с которой работают сотрудники Центра мониторинга и сотрудники группы реагирования на стороне заказчика. Карточки инцидентов создаются автоматически или вручную.

Карточки инцидента и относящаяся к инциденту информация, включая дампы трафика, файлы, образцы вредоносного кода, индикаторы компрометации и т.д., находятся в отказоустойчивом хранилище не менее трёх лет.

Из Системы сведения об инцидентах передаются в НКЦКИ через его техническую инфраструктуру.

Центр мониторинга ЗАО «ПМ»

Лицензия ФСТЭК
на мониторинг ИБ

Соглашение с 8Ц ФСБ

Год запуска — 2014

30 операторов,
исследователей,
аналитиков и инженеров

25 клиентов

28 000
подключённых узлов

353 млн событий
за 2018 год

894 инцидента
за 2018 год

<60 мин. — реагирование
на инцидент ИБ

8 000 собственных
сигнатур атак для IDS

Ссылки

- BSI Publications on Cyber-Security. Industrial Control System Security — Top 10 Threats and Countermeasures. BSI–CS005E. 2016.
- Christopher Crowley, John Pescatore. SANS Analyst Program. The Definition of SOCCess? SANS2018 Security Operations Center Survey.
- Вольфганг Шваб (Wolfgang Schwab), Матье Пужоль (Mathieu Poujol). Кибербезопасность систем промышленной автоматизации в 2018 г. По заказу Лаборатории Касперского.
- Материалы SOC-форума — soc-forum.ib-bank.ru.

Авторы

Георгий Караев

Роман Кобцев

Вячеслав Моногаров

Сергей Нейгер

Контакты

Электронная почта: gswp@amonitoring.ru

Сайт: amonitoring.ru

Телефон: +7 495 737-61-97



Приложение 1. Нормативная база

Федеральные законы

Федеральный закон от 26.07.2017 N187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Указы Президента Российской Федерации

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

Постановления правительства Российской Федерации

Постановление Правительства от 8 февраля 2018 года № 127 «О порядке категорирования объектов критической информационной инфраструктуры».

Постановление Правительства от 13 апреля 2019 года № 452 «О внесении изменений в постановление Правительства Российской Федерации от 8 февраля 2018 г. № 127».

Приказы ФСТЭК России

Приказ Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. N31 «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».

Приказ Федеральной службы по техническому и экспортному контролю от 06.12.2017 № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации».

Приказ Федеральной службы по техническому и экспортному контролю от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

Приказ Федеральной службы по техническому и экспортному контролю от 25.12.2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

Приказы ФСБ России

Приказ Федеральной службы безопасности от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам (НКЦКИ)».

Приказ Федеральной службы безопасности от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

Приказ Федеральной службы безопасности от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами КИИ РФ, между субъектами КИИ РФ и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами КИИ РФ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения».



Приказ Федеральной службы безопасности от 06.05.2019 № 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты».

Приказ Федеральной службы безопасности от 19.06.2019 № 281 «Об утверждении порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ РФ».

Приказ Федеральной службы безопасности от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов КИИ РФ».

Методические документы ФСБ России

Методические рекомендации ФСБ России по созданию ведомственных сегментов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Методические рекомендации ФСБ России по обнаружению компьютерных атак на информационные ресурсы Российской Федерации.

Методические рекомендации ФСБ России по установлению причин и ликвидации последствий компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации.

Методические рекомендации НКЦКИ по проведению мероприятий по оценке степени защищенности от компьютерных атак.

Требования к подразделениям и должностным лицам субъектов государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Регламент взаимодействия подразделений ФСБ и субъекта ГосСОПКА при осуществлении информационного обмена в области обнаружения предупреждения и ликвидации последствий компьютерных атак.

Другие документы

«Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации» (утв. Президентом РФ 03.02.2012 № 803).

«Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (утв. Президентом РФ 12.12.2014 № К 1274).