Указ 250: кто и как теперь отвечает за кибербезопасность

Рабочая тетрадь

Список нормативных актов, связанных с 250-м Указом

1. Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»
2. Постановление Правительства Российской Федерации от 15.07.2022 № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)»
3. Постановление Правительства Российской Федерации от 13.05.2022 № 860 «О проведении эксперимента по повышению уровня защищенности государственных информационных систем федеральных органов исполнительной власти и подведомственных им учреждений»
4. Распоряжение Правительства Российской Федерации от 22.06.2022 № 1661-р
5. Указ Президента Российской Федерации от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации»
6. Типовое техническое задание на выполнение работ по оценке уровня защищенности информационной инфраструктуры (https://digital.gov.ru/ru/documents/8235/)

По состоянию на 10.09.2022

А какие локальные нормативные акты по вопросам ИБ у вас есть сейчас?

А какие локальные нормативные акты по вопросам ИБ вы планируете разработать?

На кого распространяется Указ 250?

- федеральный орган исполнительной власти;
- высший исполнительный орган госвласти субъекта РФ;
- государственный фонд;
- госкорпорация (госкомпания);
- предприятие, созданное на основании федерального закона;
- стратегическое предприятие;
- стратегическое акционерное общество;
- системообразующая организация экономики (на уровне РФ или субъекта РФ);
- субъект критической информационной инфраструктуры (независимо от наличия значимых объектов КИИ) .

Всего в России более 500 тысяч организаций, попавших под действие Указа

Существуют государственные внебюджетные фонды, к которым могут быть отнесены:

- Пенсионный фонд Российской Федерации (ПФР);
- Фонд социального страхования Российской Федерации (ФСС);
- Федеральный фонд обязательного медицинскогострахования (ФФОМС);
- Территориальные фонды обязательного медицинского страхования (ТФОМС);

а также иные фонды, созданные государством, например:

- Фонд развития промышленности;
- Российский фонд прямых инвестиций;
- Российский фонд технологического развития;
- Финансовые фонды поддержки отраслей;
- Инвестиционные фонды;
- Отраслевые внебюджетные фонды НИОКР и т.п.

ВАЖНО! Попадание под действие Указа №250 не зависит от наличия значимых объектов КИИ!

Список сфер деятельности, в которых есть КИИ

1. здравоохранение
2. наука
3. транспорт
4. связь
5. энергетика
6. банковская сфера и финансовый рынок
7. топливно-энергетический комплекс
8. атомная энергетика
9. оборонная промышленность
10. ракетно-космическая промышленность
11. горнодобывающая промышленность
12. металлургическая промышленность
13. химическая промышленность
14. организации, обеспечивающи взаимодействие указанных систем и сетей

ВАЖНО! Попадание под действие Указа №250 не зависит от наличия значимых объектов КИИ!

Для заметок:

На кого распространяется Указ 250?

Единого списка системообразующих предприятий не существует – он постоянно расширяется. Например, в апреле перечень только системообразующих промышленных предприятий в РФ был расширен до 1100 организаций.

ВАЖНО! Системообразующие организации могут быть определены не только на уровне Российской Федерации, но и на уровне отдельных субъектов РФ

Перечень стратегических предприятий и стратегических акционерных обществ утвержден Указом Президента РФ от 04.08.2004 №1009 «Об утверждении Перечня стратегических предприятий и стратегических акционерных обществ»

Список госкорпораций и госкомпаний

- Агентство по страхованию вкладов
- Госкорпорация развития «ВЭБ.РФ»
- Фонд содействия реформированию жилищно-коммунального хозяйства
- Государственная корпорация по содействию разработке, производству и экспорту высокотехнологичной промышленной продукции «Ростехнологии» (Ростех)
- Государственная корпорация по атомной энергии «Росатом»
- Государственная корпорация по космической деятельности «Роскосмос»
- Государственная компания «Российские автомобильные дороги» («ГК Автодор»)
- Почта России
- РЖД
- Всероссийская государственная телевизионная и радиовещательная компания (ВГТРК)
- Газпром
- ВТБ
- Сбербанк
- Роснефть
- Объединенная авиастроительная корпорация
- Объединённая судостроительная корпорация
- Транснефть
- И д.р.

Органы управления по обеспечению информационной безопасности

- ☐ **Назначен** заместитель руководителя организации, ответственный за обеспечение ИБ.
- ☐ **Подготовлено и утверждено** положение о заместителе руководителя организации, ответственном за обеспечение ИБ, в соответствии с Постановлением Правительства РФ от 15.07.2022 № 1272.
  Примечание. Ответственным за обеспечение ИБ в субъектах РФ должен быть назначен вице-губернатор или заместитель мэра, а в министерствах — лицо в ранге заместителя министра
- ☐ Заместитель руководителя организации, ответственный за обеспечение ИБ, **входит в состав коллегиальных органов** организации.
  Примечание. Наличие коллегиального органа организации определяется уставом организации. К коллегиальным органам относятся правление, дирекция, совет директоров и т. п.
- ☐ Заместитель руководителя организации, ответственный за обеспечение ИБ, **имеет высшее образование** (не ниже уровня специалитета или магистратуры) **в сфере ИБ или прошел профпереподготовку** по программе длительностью не менее 360 часов, согласованной с ФСТЭК России или ФСБ России в соответствии с Приказом Министерства образования и науки от 19.10.2020 № 1316.
- ☐ Заместитель руководителя организации, ответственный за обеспечение ИБ, **проходит повышение квалификации** не менее одного раза в пять лет.
- ☐ Основополагающие документы организации в сфере ИТ, цифровизации и цифровой трансформации **проходят согласование** с заместителем руководителя организации, **ответственным за обеспечение ИБ**.
- ☐ Налажено регулярное информирование руководства организации о компьютерных инцидентах и текущем уровне ИБ в организации.
- ☐ Руководство организации **ознакомлено с мерами ответственности** за обеспечение ИБ (ст. 13.12, 13.12.1, 19.5 КоАП, ст. 274 и 274.1 УК РФ и др.).

Подразделение, обеспечивающее информационную безопасность

- ☐ **Создано подразделение,** отвечающее за ИБ, или эти задачи возложены на иное подразделение.
  Примечание. Часто функция обеспечения ИБ возлагается на службу информационных технологий, а подразделение ИБ входит в его состав. Однако в условиях наличия в организации еще и подразделений по цифровизации или цифровой трансформации рекомендуется в целях исключения конфликтов выделение службы ИБ в отдельное подразделение.
- ☐ **Подготовлено и утверждено** (или актуализировано) положение о подразделении, обеспечивающем ИБ, в соответствии с Постановлением Правительства РФ от 15.07.2022 № 1272.
- ☐ Подразделение **подчинено заместителю руководителя организации, ответственному за обеспечение ИБ,** или иным лицам из состава руководства организации при условии курирования со стороны руководителя организации.

Образование

Список специальностей высшего образования по ИБ

- 10.03.01 «Информационная безопасность»
- 10.05.01 «Компьютерная безопасность»
- 10.05.02 «ИБ телекоммуникационных систем»
- 10.05.03 «ИБ автоматизированных систем»
- 10.05.04 «Информационно-аналитические системы безопасности»
- 10.05.05 «Безопасность ИТ в правоохранительных органах»

ВАЖНО! Приказ Министерства образования и науки РФ №1316 от 19.10.2020 г. устанавливает срок освоения программ профессиональной переподготовки в области информационной безопасности – не менее 360 часов

Перечень организаций, осуществляющих образовательную деятельность по вопросам защиты информации, может быть найден на сайте ФСТЭК - fstec.ru > Техническая защита информации > Обучение специалистов

Positive Technologies / PT также проводит обучение по вопросам ИБ. Обращайтесь по адресу: pt@ptsecurity.com

Полезные ресурсы по обучению в ИБ

- Видеоматериалы с PHDays - phdays.com/ru/
- Видеоматериалы с The Standoff - standoff365.com/#standoff
- Материалы с RSA Conference (англ.) - rsaconference.com/library
- Материалы с BlackHat (англ.) - blackhat.com/
- Технические курсы ENISA (англ.) - enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational
- Материалы SANS (англ.) - sans.org/security-resources/
- Онлайн-курсы OpenSecurityTraining (англ.) - opensecuritytraining.info/Training.html
- Онлайн-курсы edX (англ.) - edx.org/learn/cybersecurity
- Видеолекции ФСТЭК России - bdu.fstec.ru/education
- а также курсы на Udemy, Cybrary

А какими ресурсами пользуетесь вы?

Обеспечение информационной безопасности

- ☐ **Разработана и утверждена** политика организации в области информационной безопасности.
- ☐ **Определены цели** обеспечения информационной безопасности.
- ☐ **Сформулирован перечень** недопустимых событий и негативных последствий (ущерба) для организации.
- ☐ **Проведена оценка** возможности возникновения и реализации недопустимых событий путем моделирования целевых атак.
- ☐ **Проводятся мероприятия** по недопущению и отслеживанию недопустимых событий и негативных последствий (ущерба).
- ☐ **Проводится контроль эффективности** (результативности) мероприятий по недопущению и отслеживанию недопустимых событий и негативных последствий (ущерба).
- ☐ **Реализуются** организационные и технические меры в области ИБ, требования о реализации которых направляются ФСТЭК России и ФСБ России.
- ☐ **Организованы работы** по формированию навыков и повышению осведомленности работников организации в сфере ИБ.
- ☐ **Организован контроль** за соблюдением нормативных правовых актов в области ИБ.
- ☐ **Организован контроль** пользователей организации в части соблюдения ими конфиденциальности информации и правил работы со съемными носителями информации.
- ☐ **Спланированы мероприятия** по обеспечению ИБ в подведомственных организациях, филиалах, представительствах (при их наличии).
- ☐ **Проводится контроль состояния ИБ**, включая оценку защищенности, в подведомственных организациях, филиалах, представительствах (при их наличии).
- ☐ **Проводятся регулярные практические учения** по противодействию компьютерным атакам (киберучения).
- ☐ **Проводится регулярный анализ и оценка** новых угроз, способов и методов проведения компьютерных атак (процесс threat intelligence).
- ☐ **Выстроен непрерывный процесс** выявления и устранения угроз безопасности информации и уязвимостей информационных систем, программного обеспечения и программно-аппаратных средств.
- ☐ **Проведена оценка** практической возможности использования нарушителями недостатков (уязвимостей) средств защиты информации и программного обеспечения (на примере наиболее критически важных).
- ☐ **Выстроен непрерывный процесс** обнаружения, предотвращения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

Требования ФСТЭК

1. Приказ ФСТЭК России от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

2. Приказ ФСТЭК России от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

3. Приказ ФСТЭК России от 14.03.2014 №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»

4. Приказ ФСТЭК России от 25.12.2017 №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

А также иные письма ФСТЭК

1. «О мерах по повышению защищенности информационной инфраструктуры» от 24 марта 2022 г. N 240/22/1549

2. «Об отмене плановых проверок по вопросам лицензионного контроля в 2022 году» от 14 марта 2022 г. N 240/13/1294

3. С десяток писем ограниченного доступа с рекомендациями, в т.ч. №240/22/952, №240/22/953, №240/22/960 и т.д.

Для заметок:

Приказы ФСБ по ГосСОПКЕ

1. Приказ ФСБ России от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам»

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

3. Приказ ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации...»

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

5. Приказ ФСБ России от 19.06.2019 № 281 «Об утверждении порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты...»

6. Приказ ФСБ России от 19.06.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак...»

Что-то еще? (не пишите сюда секретные приказы)

Чеклист для самопроверки

- [ ] Вы знаете, на чем зарабатывает ваша организация?

- [ ] Что остановит или замедлит операции в вашей организации?

- [ ] Что приведет к снижению прибыли / выручки / маржинальности / доли рынка вашей компании?

- [ ] Что приведет к снижению качества предоставляемого вами продукта / услуги?

- [ ] Что приведет к негативному влиянию на цель компании / бизнес-подразделения / бизнес-проекта / executive sponsor?

- [ ] Какие ключевые процессы в вашей компании?

Примерный список возможных недопустимых событий

- Кража денег со счета компании в размере 10-15% от чистой прибыли
- Непредоставление государственной услуги на 4 часа
- Демонстрация политических лозунгов на телевизионном канале
- Срыв контрактных обязательств по поставке трубопроката на 3 дня
- Недопуск болельщиков на матч крупного спортивного мероприятия
- Утечка персональных данных более 10 тысяч клиентов компании, повлекшая штраф в размере 4% от оборота
- Разлив нефтепродукта

Возможно у вас свои недопустимые события. Какие они?

Positive Technologies / PT также может помочь сформировать перечень недопустимых событий. Обращайтесь по адресу: pt@ptsecurity.com

Пример реестра недопустимых событий

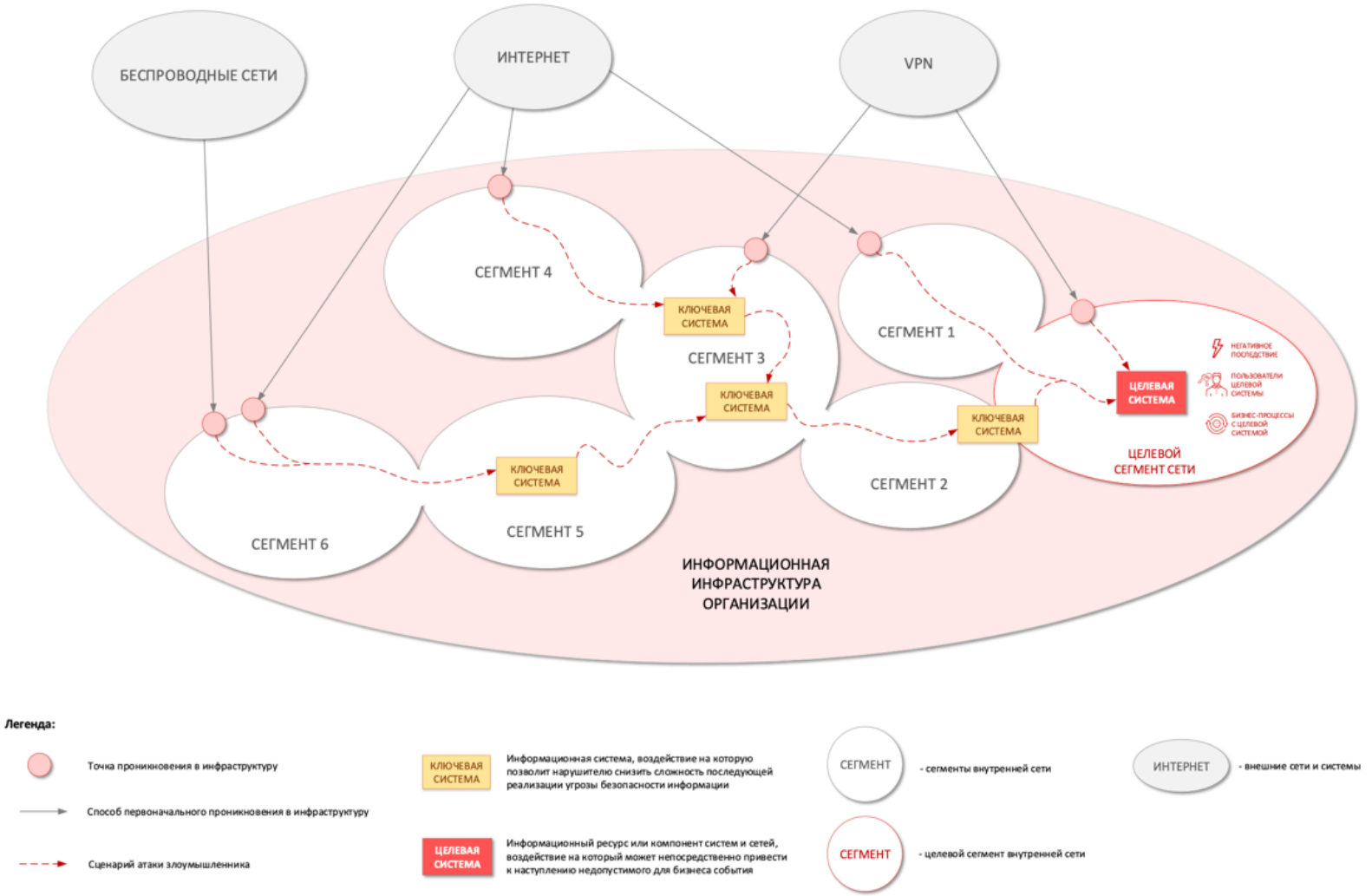
Пример реестра недопустимых событий	Сценарии реализации	Целевые системы	Критерии реализации
Утечка персональных данных более 10 тысяч клиентов компании, повлекшая штраф в размере 4% от оборота	• Несанкционированный доступ к серверу баз данных с ПДн • Кража ноутбука с ПДн • Взлом через подрядчика (supply chain attack)	• CRM-система • 1С:ERP или SAP • Система управления лояльностью	• Доступ к CRM-системе с привилегиями накопирование данных на внешний носитель • Прямой доступ к базе данных 1С или SAP, минуя доступ через приложение • Доступ к ноутбуку сотрудника отдела продаж • Доступ к резервной копии базы данных при условии отсутствия ее шифрования
Кража денег со счета компании в размере 10-15% от чистой прибыли	• Подделка реквизитов в платежном поручении • Создание ложного контрагента • Подмена суммы перевода в платежном поручении	• Банк-клиент • 1С:ERP • Каталог обмена платежными документами	• Доступ к банк-клиенту с привилегиями на создание и изменение данных в платежном поручении • Доступ к каталогу обмена с правами на запись • Доступ к 1С с правами на создание и изменение заявок на оплату • Доступ к базе данных 1С с правами на изменение платежной информации

Попробуйте составить свой реестр недопустимых событий

Недопустимое событие	Сценарии реализации	Целевые системы	Критерии реализации

Как верифицировать недопустимые события

1. Выявить точки проникновения злоумышленников
2. Выявить вектора атак
3. Выявить пути осуществления атак
4. Выявить ключевые и целевые системы
5. Выявить способы реализации атак



А какие внешние точки проникновения злоумышленников есть у вас?

- ☐ E-mail
- ☐ Web-трафик
- ☐ Site-to-Site VPN
- ☐ Remote Access VPN
- ☐ Разделяемые ресурсы (shared)
- ☐ USB-порты
- ☐ Wi-Fi
- ☐ Сайты с пиратским по (warez)
- ☐ Мобильные/BYOD-устройства
- ☐ Embedded
- ☐ Клиентское ПО (через зашифрованный канал)
- ☐ Неконтролируемые разработчики
- ☐ Подрядчики (атаки supply chain)
- ☐ Уязвимости на Web-портале
- ☐ Атака «Водопой» (поставщики обновлений ПО)
- ☐ Протокол DNS
- ☐ Облачные сервисы

Возможно, у вас есть свои внешние точки проникновения. Какие они?

Positive Technologies / PT также может помочь верифицировать ваши недопустимые события. Обращайтесь по адресу: pt@ptsecurity.com

Использование средств защиты информации

- ☐ **Проведена инвентаризация** используемых средств защиты информации и выделены все средства из недружественных государств.
  Примечание. В соответствии с Указом Президента РФ от 30.03.2022 № 166 требование о запрете использования иностранного ПО не зависит от статуса «дружественности» страны его происхождения и применяется к любому иностранному ПО, включая и средства защиты информации.

- ☐ **Проведена оценка** возможности перехода с используемых средств защиты информации из недружественных государств на иные решения (отечественные, open source или из дружественных государств).
  Примечание. В соответствии с требованиями ФСБ России и ФСТЭК России средства защиты информации, используемые на значимых объектах КИИ и в государственных информационных системах, а также средства обнаружения, предотвращения и ликвидации последствий компьютерных атак должны обладать действующей технической поддер- жкой, что может быть затруднительно в отношении решений open source.

- ☐ **Подготовлен план перехода** со средств защиты информации из недружественных государств к 1 января 2025 года.
  Примечание. В соответствии с Указом Президента РФ от 30.03.2022 года № 166 заказчикам согласно 223-ФЗ запрещена закупка любого иностранного ПО (включая и средства защиты информации) с 31 марта 2022 года независимо от статуса «дружественности» государства.

- ☐ **Осуществлено пилотирование** выбранных решений, пришедших на смену средствам защиты информации из недружественных государств.

- ☐ **Выбранные средства защиты** информации протестированы и внедрены.

Взаимодействие с ГосСОПКА

- ☐ **Подготовлен и утвержден регламент** взаимодействия с должностными лицами ФСБ России в рамках получения ими доступа, в том числе удаленного, в целях осуществления мониторинга.

- ☐ **Осуществляется мониторинг** защищенности информационных ресурсов, принадлежащих организации или используемых ею, в соответствии с порядком, утвержденным ФСБ России.

- ☐ **Организовано взаимодействие** с должностными лицами ФСБ России и ее территориальных органов по результатам мониторинга защищенности информационных ресурсов организации.

- ☐ **Организовано взаимодействие с НКЦКИ напрямую** (требуется отдельное соглашение с НКЦКИ), через аккредитацию службы ИБ в качестве центра ГосСОПКА или через взаимодействие с аккредитованными центрами ГосСОПКА.
  Примечание. Выбор способа взаимодействия с НКЦКИ определяется организацией самостоятельно.

Мы что-то забыли? Добавьте и от себя что-то!

Рекомендуем реализовать следующие защитные меры

- [ ] Выстроить процесс устранения уязвимостей и установки патчей
- [ ] Тесно контактировать с ИТ-командой, отвечающей за процесс управления патчами, и иметь актуальный список лиц, которые занимаются устранением дыр
- [ ] Мониторить внутренний трафик с помощью решений класса NTA (NDR), которые позволяют обнаруживать аномалии и угрозы, проникшие из-за периметра или инициированные изнутри, в том числе и в зашифрованном трафике

Сбалансируйте свои защитные меры (предотвращение, обнаружение и реагирование) – вместо соотношения 80-15-5 перейдите к 33-33-34

- [ ] Регулярно проводить инвентаризацию ИТ-инфраструктуры
- [ ] Поддерживать актуальную конфигурацию как сетевого оборудования, так и средств защиты
- [ ] Отслеживать изменения на Web-серверах и серверах БД и выстроить процесс контроля целостности используемого ПО и скриптов

Внедрите мониторинг своей инфраструктуры или поручите его специализированным компаниям

- [ ] Понимать риски использования злоумышленниками шифрования для скрытия своей активности и использовать решения, которые борются с этим (EDR/XDR, устройства для SSL Offload, инспекция DNS-трафика, технологии машинного обучения и т.п.)
- [ ] Контролировать ПО, полученное из третьих рук
- [ ] Отслеживать коммуникации с внешними узлами для обнаружения доступа к редко используемым или схожим по имени ресурсам

Думайте как злоумышленники – действуйте как безопасники (применяйте Red Team / Blue Team)

Список недружественных государств

Согласно распоряжению Правительства от 5 марта 2022 года №430-р и распоряжения Правительства от 23 июля 2022 года №2018-р

- Австралия
- Албания
- Андорра
- Багамские о-ва
- Великобритания (включая о. Гернси, о. Джерси и о. Мэн и подконтрольные заморские территории - о. Ангилья, Британские Виргинские острова, Гибралтар)
- Государства - члены Европейского союза
- Исландия
- Канада
- Лихтенштейн
- Микронезия
- Монако
- Новая Зеландия
- Норвегия
- Республика Корея
- Сан-Марино
- Северная Македония
- Сингапур
- Соединенные Штаты Америки
- Тайвань (Китай)
- Украина
- Черногория
- Швейцария
- Япония

А чьи решения защиты у вас сейчас?

- ☐ NGFW
- ☐ Антивирус
- ☐ Сканер уязвимостей
- ☐ COB
- ☐ NDR/NTA
- ☐ Песочница
- ☐ XDR
- ☐ SIEL
- ☐ DLP
- ☐ Прокси/SWG
- ☐ Защита e-mail
- ☐ VPN
- ☐ DAM/DCAP
- ☐ SAST/DAST
- ☐ WAF
- ☐ Другое

Полезные сайты

- НКЦКИ - cert.gov.ru
- Портал по безопасности пользователей винтернете - www.safe-surf.ru
- ФСТЭК - www.fstec.ru/
- ДИБ Банка России - www.cbr.ru/information_security/
- ДОБ Минцифры - digital.gov.ru/ru/ministry/departments/37/
- SecurityLab - securitylab.ru
- Positive Technologies - ptsecurity.com/ru-ru/

Полезные Telegram-каналы

- Технологии SOC - t.me/phd_soc
- RUSCADASEC: Кибербезопасность АСУ ТП - t.me/RUSCADASEC
- ИБ в финсекторе - t.me/FinSecurity
- Positive Technologies - t.me/Positive_Technologies
- MaxPatrol SIEM, VM & XDR - t.me/MPSIEMChat