КОД безопасности

Как выполнить требования закона № 187-ФЗ «О безопасности КИИ РФ»* с помощью продуктов «Кода безопасности»

* Федеральный закон от 26.07.2017 г. № 187-ФЗО безопасности критической информационной инфраструктуры Российской Федерации

Почему к защите критической информационной инфраструктуры (КИИ) предъявляются повышенные требования?

Уровень зависимости процессов современного предприятия от бесперебойной работы его информационных систем сегодня как никогда высок. Эпидемия вируса WannaCry, затронувшего более 500 тысяч компьютеров и парализовавшего работу сотен организаций по всему миру, атака на иранские ядерные объекты с использованием вредоносного ПО Stuxnet, атака на украинские электростанции (BlackEnergy) показали это особенно ярко. Паралич информационных систем социально значимого предприятия может оставить город/регион без воды, газа и электроэнергии. Транспортные проблемы могут привести к коллапсу целых городов.
Нарушение стабильной и бесперебойной работы систем критической информационной инфраструктуры (КИИ) не только создает угрозу здоровью и жизни людей, но и негативно влияет на экономическую, политическую и социальную устойчивость региона и государства в целом.
В новом законе о КИИ дается ясная трактовка: в случае, если объект КИИ не был защищен должным образом и ему был нанесен вред, должностные лица могут понести ответственность в соответствии с Уголовным кодексом РФ.

Какие компании являются субъектами КИИ?

Субъектами КИИ являются любые государственные или частные организации, которым принадлежат информационные системы, сети и АСУ ТП, работающие в следующих отраслях:

- Промышленность:
  - Атомная
  - Ракетно-космическая
  - Горнодобывающая
  - Металлургия
  - Химическая
  - Оборонная
- ТЭК
- Энергетика
- Здравоохранение
- Наука
- Транспорт
- Телекоммуникации
- Финансы

А также организации, обеспечивающие взаимодействие этих систем или сетей.

Что делать субъектам КИИ прямо сейчас

Для выполнения требований законодательства организациям – субъектам КИИ необходимо выполнить следующие задачи:

1. Руководитель организации – субъекта КИИ – создает комиссию по категорированию, в обязанности которой входит выявление критических процессов субъекта (управленческих, технологических, производственных и т.д.).
2. Комиссией определяются объекты КИИ – информационные системы, сети и автоматизированные системы, которые связаны с этими процессами.
3. Перечень объектов КИИ владелец (субъект КИИ) согласовывает с регулятором в установленной сфере (Минэнерго для ТЭК и нефтехимической промышленности, Министерство связи и массовых коммуникаций для телеком-операторов и т.д.) и затем отправляет в ФСТЭК России.
4. В течение года с момента согласования субъект КИИ осуществляет категорирование объектов КИИ.
   - При выборе категории объект оценивается по уровню влияния на показатели значимости. Итоговая оценка ставится по максимальному значению среди критериев.
   - Объекту могут быть присвоены три категории значимости. Либо комиссия признает, что объект КИИ не является значимым.
5. Результаты категорирования фиксируются в акте, который утверждает руководитель субъекта КИИ, далее согласовываются с отраслевым регулятором (если он установлен) и направляются в ФСТЭК России.
6. Субъект КИИ должен создать систему безопасности значимых объектов КИИ. В нее входят:
   - Люди (руководитель субъекта КИИ, уполномоченное лицо по контролю функционирования системы, сотрудники профильных структурных подразделений, сотрудники подразделений, ответственных за обеспечение безопасности)
   - Средства защиты информации
   - Организационная документация (общесистемные документы, правила безопасной работы сотрудников и регламенты действий при нештатных ситуациях)
   - Документы планирования (порядок приемки и проведения испытаний, порядок взаимодействия подразделений и т.д.)
7. Для каждого значимого объекта КИИ должны быть реализованы меры по обеспечению безопасности.

Контроль выполнения требований

После внесения в реестр объектов КИИ или после последней проверки ФСТЭК России 1 раз в 3 года проводит новую проверку объектов КИИ на соответствие требованиям законодательства.
Кроме того, субъект КИИ могут ожидать и внеплановые проверки по следующим основаниям:

- Истечение срока действия предписания об устранении нарушений требований безопасности
- Инцидент на объекте КИИ
- Поручение президента, правительства или прокуратуры

По результатам проверки возможны санкции в соответствии с действующим законодательством.
Не реже 1 раза в 5 лет осуществляется пересмотр установленной категории объекта КИИ. Также пересмотр осуществляется при следующих ситуациях:

- Реорганизация субъекта КИИ
- Изменение влияния объекта на показатели значимости
- По результатам проверки ФСТЭК России

В чем сложности защиты КИИ

Высокий уровень значимости защищаемых систем требует комплексного подхода к обеспечению информационной безопасности.
Для выполнения требований по защите КИИ систему обеспечения информационной безопасности потребуется серьезно изменить и расширить:

- К задаче потребуется привлекать не только специалистов по информационной безопасности, но и работников подразделений, эксплуатирующих объекты КИИ.
- Необходимо будет учитывать требования нескольких регуляторов в области ИБ – ФСТЭК, ФСБ, отраслевых (ЦБ для банковского сектора, Минкомсвязи России для телеком-операторов).
- Потребуется наладить постоянный мониторинг безопасности и своевременно извещать Национальный координационный центр по компьютерным инцидентам (НКЦКИ) в случае обнаружения инцидентов ИБ.

Перечисленные шаги – неполные. Комплексная система защиты должна покрывать все элементы ИТ-инфраструктуры, обеспечивать высокий уровень надежности, а также иметь удобные механизмы управления и мониторинга.

Реализация мер защиты с помощью продуктов «Кода безопасности»

Требуемые средства защиты для значимых объектов КИИ в соответствии со ст. 17 приказа ФСТЭК России №235 от 21.12.2017 и соответствующие продукты «Кода безопасности»

Требуемые средства защиты	Направление защиты	Продукты «Кода безопасности»
СЗИ от НСД	Защита рабочих станций и серверов Защита среды виртуализации	Secret Net Studio Соболь vGate
Межсетевой экран	Защита сетевой инфраструктуры Защита рабочих станций и серверов	АПКШ «Континент» Secret Net Studio
Средство обнаружения вторжений	Защита сетевой инфраструктуры Защита рабочих станций и серверов	Континент СОВ Secret Net Studio
Средства защиты каналов передачи данных	Защита сетевой инфраструктуры	АПКШ «Континент»
Средства антивирусной защиты	Защита рабочих станций и серверов	Secret Net Studio
Средства контроля защищенности		–
Средства управления событиями безопасности		–

Задачи для обеспечения безопасности значимых объектов КИИ в соответствии с требованиями ФСБ России к средствам обнаружения компьютерных атак и реагирования на инциденты ИБ

Задачи для обеспечения безопасности значимых объектов кии	Продукты «кода безопасности»
Поиск признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ	СОВ «Континент»
Криптографическая защита обмена информацией, необходимой субъектам КИИ при обнаружении, предупреждении и ликвидации последствий компьютерных атак (КА)	АПКШ «Континент»
Обнаружение КА	–
Предупреждение КА	–
Ликвидация последствий КА и реагирование на компьютерные инциденты	–

Группы мер по защите информации в соответствии с приказом ФСТЭК России №239 от 25.12.2017 и продуктовые направления «Кода безопасности»

I. Управление доступом (упд)

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Secret Net Studio	АПКШ Континент	Континент-АП + Сервер доступа	vGate	Соболь
		3	2	1	Endpoint	Network	Network	Virtualization	Endpoint
УПД.0	Разработка политики управления доступом	•	•	•	-	-	-	-	-
УПД.1	Управление учетными записями пользователей	•	•	•	+	+	+	+	+
УПД.2	Реализация политик управления доступом	•	•	•	+	+	+	+	+
УПД.3	Доверенная загрузка		•	•	-	+	+	+	+
УПД.4	Разделение полномочий (ролей) пользователей	•	•	•	+	+	+	+	+
УПД.5	Назначение минимально необходимых прав и привилегий	•	•	•	-	-	-	-	-
УПД.6	Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему	•	•	•	+	+	+	+	+
УПД.7	Предупреждение пользователя при его доступе к информационным ресурсам				-	-	-	-	+
УПД.8	Оповещение пользователя при успешном входе о предыдущем доступе к информационной (автоматизированной) системе			•	-	-	-	-	+
УПД.9	Ограничение числа параллельных сеансов доступа			•	-	+	+	-	-
УПД.10	Блокирование сеанса доступа пользователя при неактивности	•	•	•	+	+	+	+	-
УПД.11	Управление действиями пользователей до идентификации и аутентификации	•	•	•	+		+	+	-
УПД.12	Управление атрибутами безопасности				+			+	-
УПД.13	Реализация защищенного удаленного доступа	•	•	•	-	+	+	-	-
УПД.14	Контроль доступа из внешних информационных (автоматизированных) систем	•	•	•	-	-	-	-	-

II. Идентификация и аутентификация (ИАФ)

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Secret Net Studio	АПКШ Континент	Континент-АП + Сервер доступа	vGate	Соболь
		3	2	1	Endpoint	Network	Network	Virtualization	Endpoint
ИАФ.0	Разработка политики идентификации и аутентификации	•	•	•	-	-	-	-	-
ИАФ.1	Идентификация и аутентификация пользователей и инициируемых ими процессов	•	•	•	+	+	+	+	+
ИАФ.2	Идентификация и аутентификация устройств	•	•	•	+	+	+	+	-
ИАФ.3	Управление идентификаторами	•	•	•	+	+	+	+	+
ИАФ.4	Управление средствами аутентификации	•	•	•	+	+	+	+	+
ИАФ.5	Идентификация и аутентификация внешних пользователей	•	•	•	-	-	-	-	-
ИАФ.6	Двусторонняя аутентификация				+	+	+	+	-
ИАФ.7	Защита аутентификационной информации при передаче	•	•	•	+	+	+	+	+

III. Предотвращение вторжений (компьютерных атак) (СОВ)

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Secret Net Studio	АПКШ Континент	Континент-АП + Сервер доступа	vGate	Соболь
		3	2	1	Endpoint	Network	Network	Virtualization	Endpoint
СОВ.0	Разработка политики предотвращения вторжений (компьютерных атак)		•	•	-	-	-	-	-
СОВ.1	Обнаружение и предотвращение компьютерных атак		•	•	+	+	-	-	-
СОВ.2	Обновление базы решающих правил		•	•	+	+	-	-	-

IV. Обеспечение целостности (ОЦЛ)

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Secret Net Studio	АПКШ Континент	Континент-АП + Сервер доступа	vGate	Соболь
		3	2	1	Endpoint	Network	Network	Virtualization	Endpoint
ОЦЛ.0	Разработка политики обеспечения целостности	•	•	•	-	-	-	-	-
ОЦЛ.1	Контроль целостности программного обеспечения	•	•	•	+	+	+	+	+
ОЦЛ.2	Контроль целостности информации				+	-	-	+	+
ОЦЛ.3	Ограничения по вводу информации в информационную (автоматизированную) систему			•	-	-	-	+	-
ОЦЛ.4	Контроль данных, вводимых в информационную (автоматизированную) систему		•	•	-	-	-	-	-
ОЦЛ.5	Контроль ошибочных действий пользователей по вводу и (или) передаче информации и предупреждение пользователей об ошибочных действиях		•	•	-	-	-	-	-
ОЦЛ.6	Обезличивание и (или) деидентификация информации				-	-	-	-	-

V. Защита машинных носителей информации (ЗНИ)

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Secret Net Studio	АПКШ Континент	Континент-АП + Сервер доступа	vGate	Соболь
		3	2	1	Endpoint	Network	Network	Virtualization	Endpoint
ЗНИ.0	Разработка политики защиты машинных носителей информации	•	•	•	-	-	-	-	-
ЗНИ.1	Учет машинных носителей информации	•	•	•	-	-	-	-	-
ЗНИ.2	Управление физическим доступом к машинным носителям информации	•	•	•	-	-	-	-	-
ЗНИ.3	Контроль перемещения машинных носителей информации за пределы контролируемой зоны				-	-	-	-	-
ЗНИ.4	Исключение возможности несанкционированного чтения информации на машинных носителях информации				+	-	-	-	-
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации	•	•	•	+	-	-	+	-
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители информации			•	+	-	-	+	-
ЗНИ.7	Контроль подключения машинных носителей информации	•	•	•	+	-	-	+	-
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях информации	•	•	•	+	-	-	-	-

VI. Аудит безопасности (АУД)

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Secret Net Studio	АПКШ Континент	Континент-АП + Сервер доступа	vGate	Соболь
		3	2	1	Endpoint	Network	Network	Virtualization	Endpoint
АУД.0	Разработка политики аудита безопасности	•	•	•	-	-	-	-	-
АУД.1	Инвентаризация информационных ресурсов	•	•	•	-	-	-	-	-
АУД.2	Анализ уязвимостей и их устранение	•	•	•	-	-	-	-	-
АУД.3	Генерирование временных меток и (или) синхронизация системного времени	•	•	•	-	+	+	+	-
АУД.4	Регистрация событий безопасности	•	•	•	+	+	+	+	+
АУД.5	Контроль и анализ сетевого трафика			•	+	+	+	-	-
АУД.6	Защита информации о событиях безопасности	•	•	•	+	+	+	+	+
АУД.7	Мониторинг безопасности	•	•	•	+	+	+	+	+
АУД.8	Реагирование на сбои при регистрации событий безопасности	•	•	•	-	+	+	+	+
АУД.9	Анализ действий пользователей			•	+	+	+	+	-
АУД.10	Проведение внутренних аудитов	•	•	•	+	+	+	+	-
АУД.11	Проведение внешних аудитов			•	-	-	-	-	-

VII. Антивирусная защита (АВЗ)

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Secret Net Studio	АПКШ Континент	Континент-АП + Сервер доступа	vGate	Соболь
		3	2	1	Endpoint	Network	Network	Virtualization	Endpoint
АВЗ.0	Разработка политики антивирусной защиты	•	•	•	-	-	-	-	-
АВЗ.1	Реализация антивирусной защиты	•	•	•	+	-	-	-	-
АВЗ.2	Антивирусная защита электронной почты и иных сервисов	•	•	•	-	-	-	-	-
АВЗ.3	Контроль использования архивных, исполняемых и зашифрованных файлов			•	+	-	-	-	-
АВЗ.4	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	•	•	•	+	-	-	-	-
АВЗ.5	Использование средств антивирусной защиты различных производителей			•	+	-	-	-	-

VIII. Обеспечение доступности (ОДТ)

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Secret Net Studio	АПКШ Континент	Континент-АП + Сервер доступа	vGate	Соболь
		3	2	1	Endpoint	Network	Network	Virtualization	Endpoint
ОДТ.0	Разработка политики обеспечения доступности	•	•	•	-	-	-	-	-
ОДТ.1	Использование отказоустойчивых технических средств		•	•	-	+	+	-	-
ОДТ.2	Резервирование средств и систем		•	•	+	+	+	+	-
ОДТ.3	Контроль безотказного функционирования средств и систем		•	•	+	+	+	+	-
ОДТ.4	Резервное копирование информации	•	•	•	-	-	-	-	-
ОДТ.5	Обеспечение возможности восстановления информации	•	•	•	-	-	-	-	-
ОДТ.6	Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях	•	•	•	+	-	-	-	-
ОДТ.7	Кластеризация информационной (автоматизированной) системы				+	+	+	-	-
ОДТ.8	Контроль предоставляемых вычислительных ресурсов и каналов связи	•	•	•	-	-	-	-	-

IX. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Secret Net Studio	АПКШ Континент	Континент-АП + Сервер доступа	vGate	Соболь
		3	2	1	Endpoint	Network	Network	Virtualization	Endpoint
ЗИС.0	Разработка политики защиты информационной (автоматизированной) системы и ее компонентов	•	•	•	-	-	-	-	-
ЗИС.1	Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями	•	•	•	-	-	-	+	-
ЗИС.2	Защита периметра информационной (автоматизированной) системы	•	•	•	-	+	+	+	-
ЗИС.3	Эшелонированная защита информационной (автоматизированной) системы	•	•	•	-	-	-	-	-
ЗИС.4	Сегментирование информационной (автоматизированной) системы		•	•	+	+	-	+	-
ЗИС.5	Организация демилитаризованной зоны	•	•	•	-	+	-	-	-
ЗИС.6	Управление сетевыми потоками				-	+	+	+	-
ЗИС.7	Использование эмулятора среды функционирования программного обеспечения ("песочница")				-	-	-	-	-
ЗИС.8	Сокрытие архитектуры и конфигурации информационной (автоматизированной) системы	•	•	•	-	+	+	-	-
ЗИС.9	Создание гетерогенной среды				-	-	-	-	-
ЗИС.10	Использование программного обеспечения, функционирующего в средах различных операционных систем				+	-	+	-	-
ЗИС.11	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом				-	+	-	-	-
ЗИС.12	Изоляция процессов (выполнение программ) в выделенной области памяти				-	-	-	-	-
ЗИС.13	Защита неизменяемых данных		•	•	+	-	-	+	+
ЗИС.14	Использование неперезаписываемых машинных носителей информации				-	-	-	-	-
ЗИС.15	Реализация электронного почтового обмена с внешними сетями через ограниченное количество контролируемых точек				-	-	-	-	-
ЗИС.16	Защита от спама		•	•	-	-	-	-	-
ЗИС.17	Защита информации от утечек				+/-	-	-	-	-
ЗИС.18	Блокировка доступа к сайтам или типам сайтов, запрещенных к использованию				+/-	+	-	-	-

ЗИС.19	Защита информации при ее передаче по каналам связи	•	•	•	+/-	+	+	+	-
ЗИС.20	Обеспечение доверенных канала, маршрута	•	•	•	+/-	+	+	+	-
ЗИС.21	Запрет несанкционированной удаленной активации периферийных устройств	•	•	•	-	-	-	-	-
ЗИС.22	Управление атрибутами безопасности при взаимодействии с иными информационными (автоматизированными) системами				-	-	-	-	-
ЗИС.23	Контроль использования мобильного кода		•	•	+	-	-	-	-
ЗИС.24	Контроль передачи речевой информации		•	•	-	-	-	-	-
ЗИС.25	Контроль передачи видеоинформации		•	•	-	-	-	-	-
ЗИС.26	Подтверждение происхождения источника информации				-	-	-	-	-
ЗИС.27	Обеспечение подлинности сетевых соединений		•	•	+	+	+	+	-
ЗИС.28	Исключение возможности отрицания отправки информации		•	•	-	-	-	-	-
ЗИС.29	Исключение возможности отрицания получения информации		•	•	-	-	-	-	-
ЗИС.30	Использование устройств терминального доступа				+	-	-	-	-
ЗИС.31	Защита от скрытых каналов передачи информации			•	-	+	+	-	-
ЗИС.32	Защита беспроводных соединений	•	•	•	-	+	-	-	-
ЗИС.33	Исключение доступа через общие ресурсы			•	+	-	-	-	-
ЗИС.34	Защита от угроз отказа в обслуживании (DOS, DDOS-атак)	•	•	•	+	+	-	-	-
ЗИС.35	Управление сетевыми соединениями		•	•	+	+	+	-	-
ЗИС.36	Создание (эмуляция) ложных компонентов информационных (автоматизированных) систем				-	-	-	-	-
ЗИС.37	Перевод информационной (автоматизированной) системы в безопасное состояние при возникновении отказов (сбоев)				+	-	-	+	-
ЗИС.38	Защита информации при использовании мобильных устройств	•	•	•	-	-	+	-	-
ЗИС.39	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	•	•	•	-	-	-	+	-

X. Ограничение программной среды (ОПС)

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Secret Net Studio	АПКШ Континент	Континент-АП + Сервер доступа	vGate	Соболь
		3	2	1	Endpoint	Network	Network	Virtualization	Endpoint
ОПС.0	Разработка политики ограничения программной среды		•	•	-	-	-	-	-
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения			•	+	-	-	+	-
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения		•	•	-	-	-	-	-
ОПС.3	Управление временными файлами				-	-	-	-	-

XI. Защита технических средств и систем (ЗТС)

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Secret Net Studio	АПКШ Континент	Континент-АП + Сервер доступа	vGate	Соболь
		3	2	1	Endpoint	Network	Network	Virtualization	Endpoint
ЗТС.0	Разработка политики защиты технических средств и систем	•	•	•	-	-	-	-	-
ЗТС.1	Защита информации от утечки по техническим каналам				-	-	-	-	-
ЗТС.2	Организация контролируемой зоны	•	•	•	-	-	-	-	-
ЗТС.3	Управление физическим доступом	•	•	•	-	-	-	-	-
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	•	•	•	-	-	-	-	-
ЗТС.5	Защита от внешних воздействий	•	•	•	-	-	-	-	-
ЗТС.6	Маркирование аппаратных компонентов системы относительно разрешенной к обработке информации				-	-	-	-	-

XII. Реагирование на компьютерные инциденты (ИНЦ)

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Secret Net Studio	АПКШ Континент	Континент-АП + Сервер доступа	vGate	Соболь
		3	2	1	Endpoint	Network	Network	Virtualization	Endpoint
ИНЦ.0	Разработка политики реагирования на компьютерные инциденты	•	•	•	-	-	-	-	-
ИНЦ.1	Выявление компьютерных инцидентов	•	•	•	+	+	+	+	-
ИНЦ.2	Информирование о компьютерных инцидентах	•	•	•	+	+	+	+	-
ИНЦ.3	Анализ компьютерных инцидентов	•	•	•	+	+	+	+	-
ИНЦ.4	Устранение последствий компьютерных инцидентов	•	•	•	-	-	-	-	-
ИНЦ.5	Принятие мер по предотвращению повторного возникновения компьютерных инцидентов	•	•	•	-	-	-	-	-
ИНЦ.6	Хранение и защита информации о компьютерных инцидентах			•	+	+	+	+	-

XIII. Управление конфигурацией (УКФ)

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Secret Net Studio	АПКШ Континент	Континент-АП + Сервер доступа	vGate	Соболь
		3	2	1	Endpoint	Network	Network	Virtualization	Endpoint
УКФ.0	Разработка политики управления конфигурацией информационной (автоматизированной) системы	•	•	•	-	-	-	-	-
УКФ.1	Идентификация объектов управления конфигурацией				-	-	-	+	-
УКФ.2	Управление изменениями	•	•	•	-	-	-	+	-
УКФ.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения	•	•	•	+	-	-	+	-
УКФ.4	Контроль действий по внесению изменений				-	-	-	+	-

XIV. Информирование и обучение персонала (ИПО)

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Secret Net Studio	АПКШ Континент	Континент-АП + Сервер доступа	vGate	Соболь
		3	2	1	Endpoint	Network	Network	Virtualization	Endpoint
ИПО.0	Разработка политики информирования и обучения персонала	•	•	•	-	-	-	-	-
ИПО.1	Информирование персонала об угрозах безопасности информации и о правилах безопасной работы	•	•	•	-	-	-	-	-
ИПО.2	Обучение персонала правилам безопасной работы	•	•	•	-	-	-	-	-
ИПО.3	Проведение практических занятий с персоналом по правилам безопасной работы		•	•	-	-	-	-	-
ИПО.4	Контроль осведомленности персонала об угрозах безопасности информации и о правилах безопасной работы	•	•	•	-	-	-	-	-

XV. Управление обновлениями программного обеспечения (ОПО)

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Secret Net Studio	АПКШ Континент	Континент-АП + Сервер доступа	vGate	Соболь
		3	2	1	Endpoint	Network	Network	Virtualization	Endpoint
ОПО.0	Разработка политики управления обновлениями программного обеспечения	•	•	•	-	-	-	-	-
ОПО.1	Поиск, получение обновлений программного обеспечения от доверенного источника	•	•	•	-	-	-	-	-
ОПО.2	Контроль целостности обновлений программного обеспечения	•	•	•	-	-	-	-	-
ОПО.3	Тестирование обновлений программного обеспечения	•	•	•	-	-	-	-	-
ОПО.4	Установка обновлений программного обеспечения	•	•	•	+	-	-	-	-

XVI. Обеспечение действий в нештатных (непредвиденных) ситуациях (ДНС)

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Secret Net Studio	АПКШ Континент	Континент-АП + Сервер доступа	vGate	Соболь
		3	2	1	Endpoint	Network	Network	Virtualization	Endpoint
ДНС.0	Разработка политики обеспечения действий в нештатных (непредвиденных) ситуациях	•	•	•	-	-	-	-	-
ДНС.1	Разработка плана действий в нештатных ситуациях	•	•	•	-	-	-	-	-
ДНС.2	Обучение и отработка действий персонала в нештатных ситуациях	•	•	•	-	-	-	-	-
ДНС.3	Создание альтернативных мест хранения и обработки информации на случай возникновения нештатных (непредвиденных) ситуаций		•	•	-	-	-	-	-
ДНС.4	Резервирование программного обеспечения, технических средств, каналов связи на случай возникновения нештатных (непредвиденных) ситуаций		•	•	-	-	-	+	-
ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных (непредвиденных) ситуаций	•	•	•	+	+	+	+	+
ДНС.6	Анализ возникших нештатных (непредвиденных) ситуаций и принятие мер по недопущению их повторного возникновения				-	-	-	-	-

XVII. Планирование мероприятий по обеспечению безопасности (ПЛН)

Номер меры	Меры обеспечения безопасности значимого объекта	Категория значимости			Secret Net Studio	АПКШ Континент	Континент-АП + Сервер доступа	vGate	Соболь
		3	2	1	Endpoint	Network	Network	Virtualization	Endpoint
ПЛН.0	Разработка политики планирования мероприятий по обеспечению защиты информации	•	•	•	-	-	-	-	-
ПЛН.1	Разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации	•	•	•	-	-	-	-	-
ПЛН.2	Контроль выполнения мероприятий по обеспечению защиты информации	•	•	•	-	-	-	-	-

Преимущества «Кода безопасности»:

- 20-летний опыт производства продуктов для защиты систем государственной важности
- Высокий уровень сертификации
- Комплексный подход к защите инфраструктуры
- Экономия на выполнении требований нескольких регуляторов

Контакты

+7 (495) 982-30-20 (многоканальный) **info@securitycode.ru** **www.securitycode.ru**