

ПРОТОКОЛ № 3

заседания Совета по защите информации Томской области
в рамках методического сбора с государственными органами, государственными
учреждениями, юридическими лицами и (или) индивидуальными
предпринимателями, являющимися субъектами критической информационной
структуры на территории Томской области

6 июня 2018 г.

№ 165р

г. Томск

ПРЕДСЕДАТЕЛЬСТВОВАЛ управляющий делами Администрации Томской области – заместитель председателя Совета по защите информации Томской области Иванов А.А.

ПРИСУТСТВОВАЛИ:

- | | | |
|------------------|---|---|
| Иванов А.А. | – | управляющий делами Администрации Томской области – заместитель председателя Совета |
| Баев Ю.И. | – | начальник Департамента транспорта, дорожной деятельности и связи Томской области |
| Ветренко П.В. | – | директор областного государственного бюджетного учреждения «Областной центр автоматизированных информационных ресурсов Томской области» (по согласованию) |
| Кшнянкин Н.А. | – | начальник подразделения Управления Федеральной службы безопасности Российской Федерации по Томской области (по согласованию) |
| Маляр П.И. | – | председатель комитета обеспечения информационной безопасности Департамента по профилактике коррупционных и иных правонарушений Администрации Томской области – секретарь Совета |
| Максименко А.В. | – | начальник Департамента развития информационного общества Администрации Томской области |
| Маркелов С.В. | – | начальник Департамента промышленности и энергетики Администрации Томской области |
| Мысин В.И. | – | председатель Комитета общественной безопасности Администрации Томской области |
| Тимофеев С.Е. | – | начальник отдела по документальной связи и режиму Администрации Томской области |
| Толстоносов И.В. | – | заместитель Губернатора Томской области по вопросам безопасности |
| Шатурный И.Н. | – | заместитель Губернатора Томской области по промышленной политике |

ПРИГЛАШЕНЫ:

– представители организатора методического сбора с государственными органами, государственными учреждениями, юридическими лицами и (или) индивидуальными предпринимателями, являющимися субъектами критической информационной структуры – сотрудники Управления ФСТЭК России по Сибирскому федеральному округу:

Булгаков В.Н. – заместитель руководителя Управления ФСТЭК России по Сибирскому федеральному округу

Щеклачев И.В. – начальник отдела Управления ФСТЭК России по Сибирскому федеральному округу;

– участники методического сбора, являющиеся субъектами критической информационной структуры на территории Томской области, согласно списку (прилагается).

ПОВЕСТКА ДНЯ:

О выполнении требований Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» в Томской области.

СЛУШАЛИ:

Информацию заместителя руководителя Управления ФСТЭК России по Сибирскому федеральному округу Булгакова В.Н. и начальника отдела Управления ФСТЭК России по Сибирскому федеральному округу Щеклачева И.В. о выполнении требований Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (согласно Программы методического сбора по вопросам обеспечения безопасности объектов критической информационной инфраструктуры – прилагается).

РЕШИЛИ:

1. Принять к сведению и руководству в работе информацию заместителя руководителя Управления ФСТЭК России по Сибирскому федеральному округу Булгакова В.Н. и начальника отдела Управления ФСТЭК России по Сибирскому федеральному округу Щеклачева И.В. о выполнении требований Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

2. В соответствии с решением Коллегии ФСТЭК России от 24.04.2018 № 59 организациям, являющимся субъектами критической информационной инфраструктуры:

2.1. До 1 июля 2018 г. утвердить планы мероприятий по реализации Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и принятых в соответствии с ним нормативных правовых актов, предусмотрев в них в качестве первоочередных следующие мероприятия:

– создание до 10 июля 2018 г. комиссий по категорированию объектов критической информационной инфраструктуры;

- разработку до 1 августа 2018 г. перечней объектов критической информационной инфраструктуры, подлежащих категорированию, и направление информации об указанных объектах в центральный аппарат ФСТЭК России;

- создание (совершенствование созданных) до 1 сентября 2019 г. систем безопасности, включающих в том числе назначение руководящего должностного лица, ответственного за организацию и контроль обеспечения безопасности значимых объектов критической информационной инфраструктуры, создание (назначение) структурного подразделения, ответственного за обеспечение безопасности значимых объектов критической информационной инфраструктуры, а также разработку организационно-распорядительных документов по вопросам обеспечения безопасности критической информационной инфраструктуры;

- анализ и при необходимости приведение до 1 ноября 2019 г. отраслевых (ведомственных) или локальных актов, регламентирующих вопросы обеспечения информационной безопасности и защиты информации, в соответствие с Федеральным законом от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

- проведение до 1 января 2019 г. категорирования объектов критической информационной инфраструктуры в соответствии с утвержденным перечнем и направление результатов категорирования в ФСТЭК России;

- реализацию требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры с учетом установленных категорий значимости и особенностей их функционирования.

2.2. Спланировать и провести до 1 декабря 2018 г. с работниками, выполняющими функции с использованием значимых объектов критической информационной инфраструктуры, учебные занятия, в ходе которых проинформировать их о действующих требованиях по обеспечению безопасности значимых объектов критической информационной инфраструктуры и наиболее актуальных угрозах безопасности информации.

2.3. Включать в технические задания на создание (модернизацию) значимых объектов критической информационной инфраструктуры требования по обеспечению их безопасности, установленные пунктом 10 «Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры», утвержденных приказом ФСТЭК России от 25 декабря 2017 г. № 239.

2.4. Проводить на регулярной основе анализ угроз безопасности информации и уязвимостей программного обеспечения, в том числе с учетом угроз и уязвимостей, содержащихся в банке данных угроз безопасности информации (bdu.fstec.ru) и, при необходимости, принимать дополнительные меры по обеспечению безопасности значимых объектов критической информационной инфраструктуры.

2.5. Обеспечить реализацию первоочередных мер по обеспечению безопасности значимых объектов критической информационной инфраструктуры в соответствии с пунктом 22 Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, утвержденных приказом ФСТЭК России от 25 декабря 2017 г. № 239, обратив особое внимание на:

- выявление инцидентов безопасности в автоматизированных (информационных) системах и реагирование на них;

- управление конфигурацией автоматизированной (информационной) системы;
- своевременное обновление программного обеспечения с целью устранения уязвимостей в нем;
- исключение использования слабых паролей (паролей менее 6 буквенно-цифровых символов, словарных паролей типа «admin», «qwerty123», «P@swOrd» и им аналогичных);
- исключение при доступе в автоматизированные (информационные) системы и к их компонентам использование аутентификационной информации (паролей, пин-кодов), заданной по умолчанию производителями программного обеспечения и (или) используемой при настройках системы (средств) защиты информации информационной системы на этапах проектирования;
- исключение хранения конфигурационных файлов сетевого оборудования;
- обеспечение разделения функций в автоматизированной (информационной) системе по администрированию (системного администратора) и администрированию средств защиты информации (администратора безопасности), предусмотрев заведение отдельных учетных записей и разных полномочий для указанных категорий привилегированных пользователей;
- обеспечение сегментирования автоматизированной (информационной системы), как минимум, выделение в отдельный сегмент рабочих мест для управления (администрирования);
- регламентацию порядка подключения и доступа к ресурсам информационной системы мобильных устройств пользователей, исключение несанкционированных подключений мобильных устройств и беспроводных точек доступа;
- периодический контроль обеспечения уровня защищенности автоматизированных (информационных) систем.

2.6. Информацию о ходе выполнении мероприятий, перечисленных в настоящем Протоколе направить в адрес заместителя председателя Совета по защите информации Томской области до 15 сентября 2018 г.

Управляющий делами
Администрации Томской области –
заместитель председателя
Совета по защите информации Томской области

 А.А.Иванов

Председатель комитета
обеспечения информационной безопасности
Департамента по профилактике
коррупционных и иных правонарушений
Администрации Томской области –
секретарь Совета по защите информации
Томской области

 П.И.Маляр