Безопасность критической информационной инфраструктуры

Общие положения

К ключевым системам информационной инфраструктуры относятся системы, обеспечивающие управление потенциально опасными производствами или технологическими процессами на объектах, а также обеспечивающие функционирование информационно-опасных объектов, осуществляющих управление (или информационное обеспечение управления) чувствительными (важными) для государства процессами (за исключением процессов на потенциально опасных объектах).

Таким образом, понятие ключевой системы информационной инфраструктуры обобщает в себе множество различных классов информационных, автоматизированных систем и информационно-телекоммуникационных сетей (системы предупреждения и ликвидации чрезвычайных ситуаций, географические и навигационные системы, системы управления водоснабжением, энергоснабжением, транспортом и другие системы и сети).

Автоматизированные системы 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, рассматриваются как один из классов ключевых систем информационной инфраструктуры, обладающий отдельными характерными особенностями.

Приказом ФСТЭК России от 14.03.2014 № 31 определены требования к обеспечению защиты информации, обработка которой осуществляется автоматизированными системами управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (далее - автоматизированные системы управления), от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении такой информации, в том числе от деструктивных информационных воздействий (компьютерных атак), следствием которых может стать нарушение функционирования автоматизированной системы управления.

Владелец автоматизированной системы управления самостоятельно принимает решение об обеспечении защиты информации, обработка которой осуществляется этой системой и нарушение безопасности которой может привести к нарушению функционирования автоматизированной системы управления.

При обработке в автоматизированной системе управления информации, составляющей государственную тайну, ее защита обеспечивается в соответствии с законодательством Российской Федерации о государственной тайне.

Нормативные правовые акты, стандарты и рекомендации

- "Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации" (утв. Президентом РФ 12.12.2014 № К 1274)
- "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 № 195-ФЗ
- "Уголовный кодекс Российской Федерации" от 13.06.1996 № 63-ФЗ
- Информационное сообщение ФСТЭК России от 24.08.2018 № 240/25/3752 "По вопросам представления перечней объектов критической информационной инфраструктуры, подлежащих категорированию, и направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий"
- Информационное сообщение ФСТЭК России от 25.07.2014 № 240/22/2748 "По вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры в связи с изданием приказа ФСТЭК России от 14 марта 2014 г. № 31 "Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды"
- Информационное сообщение ФСТЭК России от 28.02.2018 № 240/11/879 "О методических рекомендациях по формированию аналитического прогноза по укомплектованию подразделений по обеспечению безопасности значимых объектов критической информационной инфраструктуры, противодействию иностранным техническим разведкам и технической защите информации подготовленными кадрами, утвержденных ФСТЭК России 30 сентября 2016 г."
- 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)
- Постановление Правительства РФ от 02.03.2017 № 244 "О совершенствовании требований к обеспечению надежности и безопасности электроэнергетических систем и объектов электроэнергетики и внесении изменений в некоторые акты Правительства Российской Федерации"
- Постановление Правительства РФ от 02.10.2013 № 861 "Об утверждении Правил информирования субъектами топливно-энергетического комплекса об угрозах совершения и о совершении актов незаконного вмешательства на объектах топливно-энергетического комплекса"
- Постановление Правительства РФ от 08.02.2018 № 127 "Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений"

- Постановление Правительства РФ от 17.02.2018 № 162 "Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации"
- Приказ Минздравсоцразвития России от 22.04.2009 № 205 "Об утверждении Единого квалификационного справочника должностей руководителей, специалистов и служащих, раздел "Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации"
- Приказ Минэнерго России от 06.11.2018 № 1015 "Об утверждении требований в отношении базовых (обязательных) функций и информационной безопасности объектов электроэнергетики при создании и последующей эксплуатации на территории Российской Федерации систем удаленного мониторинга и диагностики энергетического оборудования"
- Приказ ФСБ России от 24.07.2018 № 366 "О Национальном координационном центре по компьютерным инцидентам"
- 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 в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации"
- Приказ ФСБ России от 24.07.2018 № 368 "Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения"
- Приказ ФСТЭК России от 06.12.2017 № 227 "Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации"
- Приказ ФСТЭК России от 11.12.2017 № 229 "Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации"
- 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"
- Приказ ФСТЭК России от 21.12.2017 № 235 "Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования"
- Приказ ФСТЭК России от 25.12.2017 № 239 "Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации"
- Рекомендации «круглого стола» Комитета Государственной Думы по энергетике от 27.01.2017 № 3.25-5/14 на тему: «Перспективы развития вопросов информационной безопасности топливно-энергетического комплекса и законодательные аспекты обеспечения безопасности информационных систем объектов топливно-энергетического комплекса»
- Указ Президента РФ от 07.08.2004 № 1013 "Вопросы Федеральной службы охраны Российской Федерации"
- Указ Президента РФ от 11.08.2003 № 960 "Вопросы Федеральной службы безопасности Российской Федерации"
- Указ Президента РФ от 15.01.2013 № 31с "О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации" (Выписка)
- Указ Президента РФ от 16.08.2004 № 1085 "Вопросы Федеральной службы по техническому и экспортному контролю"
- Указ Президента РФ от 22.05.2015 № 260 "О некоторых вопросах информационной безопасности Российской Федерации"
- Указ Президента РФ от 22.12.2017 № 620 "О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации"
- Указ Президента РФ от 31.12.2015 № 683 "О Стратегии национальной безопасности Российской Федерации"
- Федеральный закон от 21.07.2011 № 256-ФЗ "О безопасности объектов топливно-энергетического комплекса"
- Федеральный закон от 26.07.2017 № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"
- Федеральный закон от 26.12.2008 № 294-ФЗ "О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля"

Надзорные органы

- Федеральная служба по техническому и экспортному контролю Российской Федерации
- Федеральная служба безопасности Российской Федерации

Аналитические материалы и комментарии

- Безопасность критической информационной инфраструктуры РФ
- Обзор законодательства РФ о критической информационной инфраструктуре
- Особенности режима безопасности критической информационной инфраструктуры РФ