Требования по обеспечению безопасности критической информационной инфраструктуры Российской Федерации

(Федеральный закон от 26.07.2017 № 187-ФЗ)

по состоянию на 19.06.2019

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры»
2. Указ Президента РФ от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (Выписка)
3. Указ Президента РФ от 22.12.2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»
4. 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»
5. Информационное сообщение ФСТЭК России №240/25/3752 от 24.08.2018 «По вопросам представления перечней объектов КИИ, подлежащих категорированию, и направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»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»
6. Приказ ФСТЭК России от 06.12.2017 № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации»
7. 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»
8. Приказ ФСТЭК от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»
9. Приказ ФСТЭК России от 21.12.2017 № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»;

10. Приказ ФСТЭК России от 25.12.2017 №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»
11. Приказ ФСТЭК РФ от 14 марта 2014 г. N 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»
12. Информационное сообщение ФСТЭК России №240/22/2339 от 04.05.2018 «О методических документах по вопросам обеспечения безопасности информации в КСИИ РФ»
13. Приказ ФСБ России №366 от 24.07.2018 «О НКЦКИ»
14. Приказ ФСБ России №367 от 24.07.2018 «Об утверждении Перечня информации, представляемой в ГосСОПКА и Порядка представления информации в ГосСОПКА»
15. Приказ ФСБ России №368 от 24.07.2018 «Об утверждении Порядка обмена информацией о компьютерных инцидентах и Порядка получения субъектами КИИ информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»
16. Приказ ФСБ России №196 от 06.05.2019 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»
17. Приказ ФСБ России № 281 от 19.06.2019 «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 критической информационной инфраструктуры Российской Федерации»

18. Приказ ФСБ России № 282 от 19.06.2019 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации»

РОССИЙСКАЯ ФЕДЕРАЦИЯ
ФЕДЕРАЛЬНЫЙ ЗАКОН

О БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Принят Государственной Думой 12 июля 2017 года
Одобрен Советом Федерации 19 июля 2017 года

Статья 1. Сфера действия настоящего Федерального закона

Настоящий Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее также - критическая информационная инфраструктура) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

Для целей настоящего Федерального закона используются следующие основные понятия:

1) автоматизированная система управления - комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами;

2) безопасность критической информационной инфраструктуры - состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак;

3) значимый объект критической информационной инфраструктуры - объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры;

4) компьютерная атака - целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации;

5) компьютерный инцидент - факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки;

6) критическая информационная инфраструктура - объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов;

7) объекты критической информационной инфраструктуры - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры;

8) субъекты критической информационной инфраструктуры - государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Статья 3. Правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры

1. Отношения в области обеспечения безопасности критической информационной инфраструктуры регулируются в соответствии с Конституцией Российской Федерации, общепризнанными принципами и нормами международного права, настоящим Федеральным законом, другими федеральными законами и принимаемыми в соответствии с ними иными нормативными правовыми актами.

2. Особенности применения настоящего Федерального закона к сетям связи общего пользования определяются Федеральным законом от 7 июля 2003 года N 126-ФЗ «О связи» и принимаемыми в соответствии с ним нормативными правовыми актами Российской Федерации.

Статья 4. Принципы обеспечения безопасности критической информационной инфраструктуры

Принципами обеспечения безопасности критической информационной инфраструктуры являются:

1) законность;

2) непрерывность и комплексность обеспечения безопасности критической информационной инфраструктуры, достигаемые в том числе за счет взаимодействия уполномоченных федеральных органов исполнительной власти и субъектов критической информационной инфраструктуры;

3) приоритет предотвращения компьютерных атак.

Статья 5. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

1. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации представляет собой единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. В целях настоящей статьи под информационными ресурсами Российской Федерации понимаются информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, находящиеся на территории Российской Федерации, в дипломатических представительствах и (или) консульских учреждениях Российской Федерации.

2. К силам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, относятся:

1) подразделения и должностные лица федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

2) организация, создаваемая федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, для обеспечения координации деятельности субъектов критической информационной инфраструктуры по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты (далее - национальный координационный центр по компьютерным инцидентам);

3) подразделения и должностные лица субъектов критической информационной инфраструктуры, которые принимают участие в обнаружении, предупреждении и ликвидации последствий компьютерных атак и в реагировании на компьютерные инциденты.

3. Средствами, предназначенными для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные

инциденты, являются технические, программные, программно-аппаратные и иные средства для обнаружения (в том числе для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры), предупреждения, ликвидации последствий компьютерных атак и (или) обмена информацией, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак, а также криптографические средства защиты такой информации.

4. Национальный координационный центр по компьютерным инцидентам осуществляет свою деятельность в соответствии с положением, утверждаемым федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

5. В государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации осуществляются сбор, накопление, систематизация и анализ информации, которая поступает в данную систему через средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак, информации, которая представляется субъектами критической информационной инфраструктуры и федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, в соответствии с перечнем информации и в порядке, определяемыми федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также информации, которая может представляться иными не являющимися субъектами критической информационной инфраструктуры органами и организациями, в том числе иностранными и международными.

6. Федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, организует в установленном им порядке обмен информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры, а также между субъектами критической информационной инфраструктуры и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты.

7. Предоставление из государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на

информационные ресурсы Российской Федерации сведений, составляющих государственную либо иную охраняемую законом тайну, осуществляется в соответствии с законодательством Российской Федерации.

Статья 6. Полномочия Президента Российской Федерации и органов государственной власти Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры

1. Президент Российской Федерации определяет:

1) основные направления государственной политики в области обеспечения безопасности критической информационной инфраструктуры;

2) федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

3) федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

4) порядок создания и задачи государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

2. Правительство Российской Федерации устанавливает:

1) показатели критериев значимости объектов критической информационной инфраструктуры и их значения, а также порядок и сроки осуществления их категорирования;

2) порядок осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры;

3) порядок подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры.

3. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации:

1) вносит предложения о совершенствовании нормативно-правового регулирования в области обеспечения безопасности критической информационной инфраструктуры Президенту Российской Федерации и (или) в Правительство Российской Федерации;

2) утверждает порядок ведения реестра значимых объектов критической информационной инфраструктуры и ведет данный реестр;

3) утверждает форму направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий;

4) устанавливает требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры (требования по обеспечению безопасности информационно-телекоммуникационных сетей, которым присвоена одна из категорий значимости и которые включены в реестр значимых объектов критической информационной инфраструктуры, устанавливаются по согласованию с федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в области связи), а также требования к созданию систем безопасности таких объектов и обеспечению их функционирования (в банковской сфере и в иных сферах финансового рынка устанавливает указанные требования по согласованию с Центральным банком Российской Федерации);

5) осуществляет государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, а также утверждает форму акта проверки, составляемого по итогам проведения указанного контроля.

4. Федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации:

1) вносит предложения о совершенствовании нормативно-правового регулирования в области обеспечения безопасности критической информационной инфраструктуры Президенту Российской Федерации и (или) в Правительство Российской Федерации;

2) создает национальный координационный центр по компьютерным инцидентам и утверждает положение о нем;

3) координирует деятельность субъектов критической информационной инфраструктуры по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

4) организует и проводит оценку безопасности критической информационной инфраструктуры;

5) определяет перечень информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, и порядок ее представления;

6) утверждает порядок информирования федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры (в банковской сфере и в иных сферах финансового рынка утверждает указанный порядок по согласованию с Центральным банком Российской Федерации);

7) утверждает порядок обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры, между субъектами критической информационной инфраструктуры и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, а также порядок получения субъектами критической информационной инфраструктуры информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения;

8) организует установку на значимых объектах критической информационной инфраструктуры и в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры, средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

9) устанавливает требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

10) утверждает порядок, технические условия 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 критической информационной инфраструктуры (в банковской сфере и в иных сферах финансового рынка утверждает указанные порядок и технические условия по согласованию с Центральным банком Российской Федерации).

5. Федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в области связи, утверждает по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, порядок, технические условия установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры.

Статья 7. Категорирование объектов критической информационной инфраструктуры

1. Категорирование объекта критической информационной инфраструктуры представляет собой установление соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их

значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения.

2. Категорирование осуществляется исходя из:

1) социальной значимости, выражающейся в оценке возможного ущерба, причиняемого жизни или здоровью людей, возможности прекращения или нарушения функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, а также максимальном времени отсутствия доступа к государственной услуге для получателей такой услуги;

2) политической значимости, выражающейся в оценке возможного причинения ущерба интересам Российской Федерации в вопросах внутренней и внешней политики;

3) экономической значимости, выражающейся в оценке возможного причинения прямого и косвенного ущерба субъектам критической информационной инфраструктуры и (или) бюджетам Российской Федерации;

4) экологической значимости, выражающейся в оценке уровня воздействия на окружающую среду;

5) значимости объекта критической информационной инфраструктуры для обеспечения обороны страны, безопасности государства и правопорядка.

3. Устанавливаются три категории значимости объектов критической информационной инфраструктуры - первая, вторая и третья.

4. Субъекты критической информационной инфраструктуры в соответствии с критериями значимости и показателями их значений, а также порядком осуществления категорирования присваивают одну из категорий значимости принадлежащим им на праве собственности, аренды или ином законном основании объектам критической информационной инфраструктуры. Если объект критической информационной инфраструктуры не соответствует критериям значимости, показателям этих критериев и их значениям, ему не присваивается ни одна из таких категорий.

5. Сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий субъекты критической информационной инфраструктуры в письменном виде в десятидневный срок со дня принятия ими соответствующего решения направляют в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, по утвержденной им форме.

6. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, в тридцатидневный срок со дня получения сведений, указанных в части 5 настоящей статьи, проверяет соблюдение порядка осуществления категорирования и правильность присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо неприсвоения ему ни одной из таких категорий.

7. В случае, если субъектом критической информационной инфраструктуры соблюден порядок осуществления категорирования и принадлежащему ему на праве собственности, аренды или ином законном основании объекту критической информационной инфраструктуры правильно присвоена одна из категорий значимости, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, вносит сведения о таком объекте критической информационной инфраструктуры в реестр значимых объектов критической информационной инфраструктуры, о чем в десятидневный срок уведомляется субъект критической информационной инфраструктуры.

8. В случае, если федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, выявлены нарушения порядка осуществления категорирования и (или) объекту критической информационной инфраструктуры, принадлежащему на праве собственности, аренды или ином законном основании субъекту критической информационной инфраструктуры, неправильно присвоена одна из категорий значимости и (или) необоснованно не присвоена ни одна из таких категорий и (или) субъектом критической информационной инфраструктуры представлены неполные и (или) недостоверные сведения о результатах присвоения такому объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, в десятидневный срок со дня поступления представленных сведений возвращает их в письменном виде субъекту критической информационной инфраструктуры с мотивированным обоснованием причин возврата.

9. Субъект критической информационной инфраструктуры после получения мотивированного обоснования причин возврата сведений, указанных в части 5 настоящей статьи, не более чем в десятидневный срок устраняет отмеченные недостатки и повторно направляет такие сведения в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

10. Сведения об отсутствии необходимости присвоения объекту критической информационной инфраструктуры одной из категорий значимости после их проверки направляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, о чем в десятидневный срок уведомляется субъект критической информационной инфраструктуры.

11. В случае непредставления субъектом критической информационной инфраструктуры сведений, указанных в части 5 настоящей статьи, федеральный

орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, направляет в адрес указанного субъекта требование о необходимости соблюдения положений настоящей статьи.

12. Категория значимости, к которой отнесен значимый объект критической информационной инфраструктуры, может быть изменена в порядке, предусмотренном для категорирования, в следующих случаях:

1) по мотивированному решению федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, принятому по результатам проверки, проведенной в рамках осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры;

2) в случае изменения значимого объекта критической информационной инфраструктуры, в результате которого такой объект перестал соответствовать критериям значимости и показателям их значений, на основании которых ему была присвоена определенная категория значимости;

3) в связи с ликвидацией, реорганизацией субъекта критической информационной инфраструктуры и (или) изменением его организационно-правовой формы, в результате которых были изменены либо утрачены признаки субъекта критической информационной инфраструктуры.

Статья 8. Реестр значимых объектов критической информационной инфраструктуры

1. В целях учета значимых объектов критической информационной инфраструктуры федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, ведет реестр значимых объектов критической информационной инфраструктуры в установленном им порядке. В данный реестр вносятся следующие сведения:

1) наименование значимого объекта критической информационной инфраструктуры;

2) наименование субъекта критической информационной инфраструктуры;

3) сведения о взаимодействии значимого объекта критической информационной инфраструктуры и сетей электросвязи;

4) сведения о лице, эксплуатирующем значимый объект критической информационной инфраструктуры;

5) категория значимости, которая присвоена значимому объекту критической информационной инфраструктуры;

6) сведения о программных и программно-аппаратных средствах, используемых на значимом объекте критической информационной инфраструктуры;

7) меры, применяемые для обеспечения безопасности значимого объекта критической информационной инфраструктуры.

2. Сведения из реестра значимых объектов критической информационной инфраструктуры направляются в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

3. В случае утраты значимым объектом критической информационной инфраструктуры категории значимости он исключается федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, из реестра значимых объектов критической информационной инфраструктуры.

Статья 9. Права и обязанности субъектов критической информационной инфраструктуры

1. Субъекты критической информационной инфраструктуры имеют право:

1) получать от федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, информацию, необходимую для обеспечения безопасности значимых объектов критической информационной инфраструктуры, принадлежащих им на праве собственности, аренды или ином законном основании, в том числе об угрозах безопасности обрабатываемой такими объектами информации и уязвимости программного обеспечения, оборудования и технологий, используемых на таких объектах;

2) в порядке, установленном федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, получать от указанного органа информацию о средствах и способах проведения компьютерных атак, а также о методах их предупреждения и обнаружения;

3) при наличии согласия федерального органа исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, за свой счет приобретать, арендовать, устанавливать и обслуживать средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

4) разрабатывать и осуществлять мероприятия по обеспечению безопасности значимого объекта критической информационной инфраструктуры.

2. Субъекты критической информационной инфраструктуры обязаны:

1) незамедлительно информировать о компьютерных инцидентах федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на

информационные ресурсы Российской Федерации, а также Центральный банк Российской Федерации (в случае, если субъект критической информационной инфраструктуры осуществляет деятельность в банковской сфере и в иных сферах финансового рынка) в установленном указанным федеральным органом исполнительной власти порядке (в банковской сфере и в иных сферах финансового рынка указанный порядок устанавливается по согласованию с Центральным банком Российской Федерации);

2) оказывать содействие должностным лицам федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов;

3) в случае установки на объектах критической информационной инфраструктуры средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, обеспечивать выполнение порядка, технических условий установки и эксплуатации таких средств, их сохранность.

3. Субъекты критической информационной инфраструктуры, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, наряду с выполнением обязанностей, предусмотренных частью 2 настоящей статьи, также обязаны:

1) соблюдать требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленные федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

2) выполнять предписания должностных лиц федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, об устранении нарушений в части соблюдения требований по обеспечению безопасности значимого объекта критической информационной инфраструктуры, выданные этими лицами в соответствии со своей компетенцией;

3) реагировать на компьютерные инциденты в порядке, утвержденном федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, принимать меры по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры;

4) обеспечивать беспрепятственный доступ должностным лицам федерального органа исполнительной власти, уполномоченного в области

обеспечения безопасности критической информационной инфраструктуры Российской Федерации, к значимым объектам критической информационной инфраструктуры при реализации этими лицами полномочий, предусмотренных статьей 13 настоящего Федерального закона.

Статья 10. Система безопасности значимого объекта критической информационной инфраструктуры

1. В целях обеспечения безопасности значимого объекта критической информационной инфраструктуры субъект критической информационной инфраструктуры в соответствии с требованиями к созданию систем безопасности таких объектов и обеспечению их функционирования, утвержденными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, создает систему безопасности такого объекта и обеспечивает ее функционирование.

2. Основными задачами системы безопасности значимого объекта критической информационной инфраструктуры являются:

1) предотвращение неправомерного доступа к информации, обрабатываемой значимым объектом критической информационной инфраструктуры, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;

2) недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта критической информационной инфраструктуры;

3) восстановление функционирования значимого объекта критической информационной инфраструктуры, обеспечиваемого в том числе за счет создания и хранения резервных копий необходимой для этого информации;

4) непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Статья 11. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры

1. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, устанавливаемые федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, дифференцируются в зависимости от категории значимости объектов критической информационной инфраструктуры и этими требованиями предусматриваются:

1) планирование, разработка, совершенствование и осуществление внедрения мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры;

2) принятие организационных и технических мер для обеспечения безопасности значимых объектов критической информационной инфраструктуры;

3) установление параметров и характеристик программных и программно-аппаратных средств, применяемых для обеспечения безопасности значимых объектов критической информационной инфраструктуры.

2. Государственные органы и российские юридические лица, выполняющие функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере деятельности, по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, могут устанавливать дополнительные требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, содержащие особенности функционирования таких объектов в установленной сфере деятельности.

Статья 12. Оценка безопасности критической информационной инфраструктуры

1. Оценка безопасности критической информационной инфраструктуры осуществляется федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, в целях прогнозирования возникновения возможных угроз безопасности критической информационной инфраструктуры и выработки мер по повышению устойчивости ее функционирования при проведении в отношении ее компьютерных атак.

2. При осуществлении оценки безопасности критической информационной инфраструктуры проводится анализ:

1) данных, получаемых при использовании средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, в том числе информации о наличии в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры, признаков компьютерных атак;

2) информации, представляемой субъектами критической информационной инфраструктуры и федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, в соответствии с перечнем информации и в порядке, определяемыми федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы

Российской Федерации, а также иными не являющимися субъектами критической информационной инфраструктуры органами и организациями, в том числе иностранными и международными;

3) сведений, представляемых в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, о нарушении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, в результате которого создаются предпосылки возникновения компьютерных инцидентов;

4) иной информации, получаемой федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, в соответствии с законодательством Российской Федерации.

3. Для реализации положений, предусмотренных частями 1 и 2 настоящей статьи, федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, организует установку в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры, средств, предназначенных для поиска признаков компьютерных атак в таких сетях электросвязи.

4. В целях разработки мер по совершенствованию безопасности критической информационной инфраструктуры федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, направляет в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, результаты осуществления оценки безопасности критической информационной инфраструктуры.

Статья 13. Государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры

1. Государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры проводится в целях проверки соблюдения субъектами критической информационной инфраструктуры, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, требований, установленных настоящим Федеральным законом и

принятыми в соответствии с ним нормативными правовыми актами. Указанный государственный контроль проводится путем осуществления федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, плановых или внеплановых проверок.

2. Основанием для осуществления плановой проверки является истечение трех лет со дня:

1) внесения сведений об объекте критической информационной инфраструктуры в реестр значимых объектов критической информационной инфраструктуры;

2) окончания осуществления последней плановой проверки в отношении значимого объекта критической информационной инфраструктуры.

3. Основанием для осуществления внеплановой проверки является:

1) истечение срока выполнения субъектом критической информационной инфраструктуры выданного федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, предписания об устранении выявленного нарушения требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры;

2) возникновение компьютерного инцидента, повлекшего негативные последствия, на значимом объекте критической информационной инфраструктуры;

3) приказ (распоряжение) руководителя федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, изданный в соответствии с поручением Президента Российской Федерации или Правительства Российской Федерации либо на основании требования прокурора об осуществлении внеплановой проверки в рамках проведения надзора за исполнением законов по поступившим в органы прокуратуры материалам и обращениям.

4. По итогам плановой или внеплановой проверки федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, составляется акт проверки по утвержденной указанным органом форме.

5. На основании акта проверки в случае выявления нарушения требований настоящего Федерального закона и принятых в соответствии с ним нормативных правовых актов по обеспечению безопасности значимых объектов критической информационной инфраструктуры федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, выдает субъекту критической информационной инфраструктуры предписание об устранении выявленного нарушения с указанием сроков его устранения.

Статья 14. Ответственность за нарушение требований настоящего Федерального закона и принятых в соответствии с ним иных нормативных правовых актов

Нарушение требований настоящего Федерального закона и принятых в соответствии с ним иных нормативных правовых актов влечет за собой ответственность в соответствии с законодательством Российской Федерации.

Статья 15. Вступление в силу настоящего Федерального закона

Настоящий Федеральный закон вступает в силу с 1 января 2018 года.

Президент
Российской Федерации В.ПУТИН

Москва, Кремль
26 июля 2017 года
N 187-ФЗ

УКАЗ
ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О СОЗДАНИИ ГОСУДАРСТВЕННОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ, ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

(Выписка)

В целях обеспечения информационной безопасности Российской Федерации постановляю:

1. Возложить на Федеральную службу безопасности Российской Федерации полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации - информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом.

2. Определить основными задачами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации:

а) прогнозирование ситуации в области обеспечения информационной безопасности Российской Федерации;

б) обеспечение взаимодействия владельцев информационных ресурсов Российской Федерации, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак;

в) осуществление контроля степени защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак;

г) установление причин компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации.

3. Установить, что Федеральная служба безопасности Российской Федерации:

а) организует и проводит работы по созданию государственной системы, названной в пункте 1 настоящего Указа, осуществляет контроль за исполнением этих работ, а также обеспечивает во взаимодействии с государственными органами функционирование ее элементов;

б) разрабатывает методику обнаружения компьютерных атак на информационные системы и информационно-телекоммуникационные сети государственных органов и по согласованию с их владельцами - на иные информационные системы и информационно-телекоммуникационные сети;

в) определяет порядок обмена информацией между федеральными органами исполнительной власти о компьютерных инцидентах, связанных с функционированием информационных ресурсов Российской Федерации;

г) организует и проводит в соответствии с законодательством Российской Федерации мероприятия по оценке степени защищенности критической информационной инфраструктуры Российской Федерации от компьютерных атак;

д) разрабатывает методические рекомендации по организации защиты критической информационной инфраструктуры Российской Федерации от компьютерных атак;

е) определяет порядок обмена информацией между федеральными органами исполнительной власти и уполномоченными органами иностранных государств

(международными организациями) о компьютерных инцидентах, связанных с функционированием информационных ресурсов, и организует обмен такой информацией.

4. Настоящий Указ вступает в силу со дня его подписания.

Президент
Российской Федерации В.ПУТИН

Москва, Кремль
15 января 2013 года
N 31с

22 декабря 2017 года N 620

УКАЗ
ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ

О СОВЕРШЕНСТВОВАНИИ ГОСУДАРСТВЕННОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ, ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

В целях совершенствования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и в соответствии со статьей 6 Федерального закона от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» постановляю:

1. Возложить на Федеральную службу безопасности Российской Федерации функции федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации - информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, находящиеся на территории Российской Федерации, в дипломатических представительствах и консульских учреждениях Российской Федерации.

2. Установить, что задачами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации являются:

а) прогнозирование ситуации в области обеспечения информационной безопасности Российской Федерации;

б) обеспечение взаимодействия владельцев информационных ресурсов Российской Федерации, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак;

в) осуществление контроля степени защищенности информационных ресурсов Российской Федерации от компьютерных атак;

г) установление причин компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации.

3. Установить, что Федеральная служба безопасности Российской Федерации:

а) обеспечивает и контролирует функционирование государственной системы, названной в пункте 1 настоящего Указа;

б) формирует и реализует в пределах своих полномочий государственную научно-техническую политику в области обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

в) разрабатывает методические рекомендации:

по обнаружению компьютерных атак на информационные ресурсы Российской Федерации;

по предупреждению и установлению причин компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации, а также по ликвидации последствий этих инцидентов.

4. Внести в пункт 9 Положения о Федеральной службе безопасности Российской Федерации, утвержденного Указом Президента Российской Федерации от 11 августа 2003 г. N 960 «Вопросы Федеральной службы безопасности Российской Федерации» (Собрание законодательства Российской Федерации, 2003, N 33, ст. 3254; 2004, N 28, ст. 2883; 2005, N 36, ст. 3665; N 49, ст. 5200; 2006, N 25, ст. 2699; N 31, ст. 3463; 2007, N 1, ст. 205; N 49, ст. 6133; N

53, ст. 6554; 2008, N 36, ст. 4087; N 43, ст. 4921; N 47, ст. 5431; 2010, N 17, ст. 2054; N 20, ст. 2435; 2011, N 2, ст. 267; N 9, ст. 1222; 2012, N 7, ст. 818; N 8, ст. 993; N 32, ст. 4486; 2013, N 12, ст. 1245; N 26, ст. 3314; N 52, ст. 7137, 7139; 2014, N 10, ст. 1020; N 44, ст. 6041; 2015, N 4, ст. 641; 2016, N 50, ст. 7077; 2017, N 21, ст. 2991), следующие изменения:

а) подпункт 20.1 изложить в следующей редакции:

«20.1) в пределах своих полномочий разрабатывает и утверждает нормативные и методические документы по вопросам обеспечения информационной безопасности информационных систем, созданных с использованием суперкомпьютерных и грид-технологий, информационных ресурсов Российской Федерации, а также осуществляет контроль за обеспечением информационной безопасности указанных систем и ресурсов;»;

б) подпункт 47 изложить в следующей редакции:

«47) организует и проводит исследования в области защиты информации, экспертные криптографические, инженерно-криптографические и специальные исследования шифровальных средств, специальных и закрытых информационно-телекоммуникационных систем, информационных систем, созданных с использованием суперкомпьютерных и грид-технологий, а также информационных ресурсов Российской Федерации;»;

в) подпункт 49 изложить в следующей редакции:

«49) осуществляет подготовку экспертных заключений на предложения о проведении работ по созданию специальных и защищенных с использованием шифровальных (криптографических) средств информационно-телекоммуникационных систем и сетей связи, информационных систем, созданных с использованием суперкомпьютерных и грид-технологий, а также информационных ресурсов Российской Федерации;».

5. Внести в Указ Президента Российской Федерации от 15 января 2013 г. N 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (Собрание законодательства Российской Федерации, 2013, N 3, ст. 178) следующие изменения:

а) из пункта 1 слова «- информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом» исключить;

б) пункт 2 и подпункты «а» - «е» пункта 3 признать утратившими силу.

6. Настоящий Указ вступает в силу с 1 января 2018 г.

Президент
Российской Федерации В.ПУТИН

Москва, Кремль
22 декабря 2017 года
N 620

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ
от 8 февраля 2018 г. N 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

В соответствии с пунктом 1 части 2 статьи 6 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» Правительство Российской Федерации постановляет:

1. Утвердить прилагаемые:

Правила категорирования объектов критической информационной инфраструктуры Российской Федерации;

перечень показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений.

2. Финансирование расходов, связанных с реализацией настоящего постановления государственными органами и государственными учреждениями, осуществляется за счет и в пределах бюджетных ассигнований, предусмотренных соответствующим бюджетом на обеспечение деятельности субъектов критической информационной инфраструктуры.

Председатель Правительства
Российской Федерации Д.МЕДВЕДЕВ

Утверждены
постановлением Правительства
Российской Федерации
от 8 февраля 2018 г. N 127

ПРАВИЛА
КАТЕГОРИРОВАНИЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

1. Настоящие Правила устанавливают порядок и сроки категорирования объектов критической информационной инфраструктуры Российской Федерации (далее соответственно - критическая информационная инфраструктура, категорирование).

2. Категорирование осуществляется субъектами критической информационной инфраструктуры в отношении принадлежащих им на праве собственности, аренды или ином законном основании объектов критической информационной инфраструктуры.

3. Категорированию подлежат объекты критической информационной инфраструктуры, которые обеспечивают управленческие, технологические, производственные, финансово-экономические и (или) иные процессы в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры.

4. Определение категорий значимости объектов критической информационной инфраструктуры (далее - категория значимости) осуществляется на основании показателей критериев значимости объектов критической информационной инфраструктуры и их значений, предусмотренных перечнем показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений, утвержденным постановлением Правительства Российской Федерации от 8 февраля 2018 г. N 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» (далее соответственно - перечень показателей критериев значимости, показатели критериев значимости).

5. Категорирование включает в себя:

а) определение процессов, указанных в пункте 3 настоящих Правил, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры;

б) выявление управленческих, технологических, производственных, финансово-экономических и (или) иных процессов в рамках выполнения функций (полномочий) или осуществления видов деятельности субъектов критической информационной инфраструктуры, нарушение и (или) прекращение которых может привести к негативным социальным, политическим, экономическим, экологическим последствиям, последствиям для обеспечения обороны страны, безопасности государства и правопорядка (далее - критические процессы);

в) определение объектов критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов;

г) формирование перечня объектов критической информационной инфраструктуры, подлежащих категорированию (далее - перечень объектов);

д) оценку в соответствии с перечнем показателей критериев значимости масштаба возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры;

е) присвоение каждому из объектов критической информационной инфраструктуры одной из категорий значимости либо принятие решения об отсутствии необходимости присвоения им одной из категорий значимости.

6. Объекту критической информационной инфраструктуры по результатам категорирования присваивается в соответствии с перечнем показателей критериев значимости категория значимости с наивысшим значением.

Для каждого показателя критериев значимости, для которого установлено более одного значения такого показателя (территория, количество людей), оценка производится по каждому из значений показателя критериев значимости, а категория значимости присваивается по наивысшему значению такого показателя.

В случае если ни один из показателей критериев значимости неприменим для объекта критической информационной инфраструктуры или объект критической информационной инфраструктуры не соответствует ни одному показателю критериев значимости и их значениям, категория значимости не присваивается.

7. Устанавливаются 3 категории значимости. Самая высокая категория - первая, самая низкая - третья.

8. В отношении объекта критической информационной инфраструктуры, создаваемого в рамках создания объекта капитального строительства, категория значимости определяется при формировании заказчиком, техническим заказчиком или застройщиком требований к объекту критической информационной инфраструктуры с учетом имеющихся исходных данных о критических процессах субъекта критической информационной инфраструктуры.

Для создаваемого объекта критической информационной инфраструктуры, указанного в абзаце первом настоящего пункта, категория значимости может быть уточнена в ходе его проектирования.

9. Для объектов, принадлежащих одному субъекту критической информационной инфраструктуры, но используемых для целей контроля и управления технологическим и (или) производственным оборудованием, принадлежащим другому субъекту критической информационной инфраструктуры, категорирование осуществляется на основе исходных данных, представляемых субъектом критической информационной инфраструктуры, которому принадлежит технологическое и (или) производственное оборудование.

10. Исходными данными для категорирования являются:

а) сведения об объекте критической информационной инфраструктуры (назначение, архитектура объекта, применяемые программные и программно-аппаратные средства, взаимодействие с другими объектами критической информационной инфраструктуры, наличие и характеристики доступа к сетям связи);

б) процессы, указанные в пункте 3 настоящих Правил, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры;

в) состав информации, обрабатываемой объектами критической информационной инфраструктуры, сервисы по управлению, контролю или мониторингу, предоставляемые объектами критической информационной инфраструктуры;

г) декларация промышленной безопасности опасного производственного объекта, декларация безопасности гидротехнического сооружения и паспорт объекта топливно-энергетического комплекса в случае, если на указанных объектах функционирует объект критической информационной инфраструктуры (если разработка указанных деклараций и паспорта предусмотрена законодательством Российской Федерации);

д) сведения о взаимодействии объекта критической информационной инфраструктуры с другими объектами критической информационной инфраструктуры и (или) о зависимости функционирования объекта критической информационной инфраструктуры от других таких объектов;

е) угрозы безопасности информации в отношении объекта критической информационной инфраструктуры, а также имеющиеся данные, в том числе статистические, о компьютерных инцидентах, произошедших ранее на объектах критической информационной инфраструктуры соответствующего типа.

11. Для проведения категорирования решением руководителя субъекта критической информационной инфраструктуры создается комиссия по категорированию, в состав которой включаются:

а) руководитель субъекта критической информационной инфраструктуры или уполномоченное им лицо;

б) работники субъекта критической информационной инфраструктуры, являющиеся специалистами в области выполняемых функций или осуществляемых видов деятельности, и в области информационных технологий и связи, а также специалисты по эксплуатации основного технологического оборудования, технологической (промышленной) безопасности, контролю за опасными веществами и материалами, учету опасных веществ и материалов;

в) работники субъекта критической информационной инфраструктуры, на которых возложены функции обеспечения безопасности (информационной безопасности) объектов критической информационной инфраструктуры;

г) работники подразделения по защите государственной тайны субъекта критической информационной инфраструктуры (в случае, если объект критической информационной инфраструктуры обрабатывает информацию, составляющую государственную тайну);

д) работники структурного подразделения по гражданской обороне и защите от чрезвычайных ситуаций или работники, уполномоченные на решение задач в области гражданской обороны и защиты от чрезвычайных ситуаций.

12. В состав комиссии по категорированию могут включаться представители государственных органов и российских юридических лиц, выполняющих функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере деятельности, по согласованию с государственными органами и российскими юридическими лицами.

13. Комиссию по категорированию возглавляет руководитель субъекта критической информационной инфраструктуры или уполномоченное им лицо.

14. Комиссия по категорированию в ходе своей работы:

а) определяет процессы, указанные в пункте 3 настоящих Правил, в рамках выполнения функций (полномочий) или осуществления видов деятельности субъекта критической информационной инфраструктуры;

б) выявляет наличие критических процессов у субъекта критической информационной инфраструктуры;

в) выявляет объекты критической информационной инфраструктуры, которые обрабатывают информацию, необходимую для обеспечения выполнения критических процессов, и (или) осуществляют управление, контроль или мониторинг критических процессов, а также готовит предложения для включения в перечень объектов;

г) рассматривает возможные действия нарушителей в отношении объектов критической информационной инфраструктуры, а также иные источники угроз безопасности информации;

д) анализирует угрозы безопасности информации и уязвимости, которые могут привести к возникновению компьютерных инцидентов на объектах критической информационной инфраструктуры;

е) оценивает в соответствии с перечнем показателей критериев значимости масштаб возможных последствий в случае возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры;

ж) устанавливает каждому из объектов критической информационной инфраструктуры одну из категорий значимости либо принимает решение об отсутствии необходимости присвоения им категорий значимости.

15. Перечень объектов утверждается субъектом критической информационной инфраструктуры. Перечень объектов подлежит согласованию с государственным органом или российским юридическим лицом, выполняющим функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в

установленной сфере в части подведомственных им субъектов критической информационной инфраструктуры.

Максимальный срок категорирования не должен превышать одного года со дня утверждения субъектом критической информационной инфраструктуры перечня объектов.

Перечень объектов в течение 5 рабочих дней после утверждения направляется в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры.

16. Решение комиссии по категорированию оформляется актом, который должен содержать сведения об объекте критической информационной инфраструктуры, результаты анализа угроз безопасности информации объекта критической информационной инфраструктуры, реализованные меры по обеспечению безопасности объекта критической информационной инфраструктуры, сведения о присвоенной объекту критической информационной инфраструктуры категории значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, а также сведения о необходимых мерах по обеспечению безопасности в соответствии с требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры.

Акт подписывается членами комиссии по категорированию и утверждается руководителем субъекта критической информационной инфраструктуры.

Субъект критической информационной инфраструктуры обеспечивает хранение акта до вывода из эксплуатации объекта критической информационной инфраструктуры или до изменения категории значимости.

17. Субъект критической информационной инфраструктуры в течение 10 дней со дня утверждения акта, указанного в пункте 16 настоящих Правил, направляет в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий. Указанные сведения включают:

а) сведения об объекте критической информационной инфраструктуры;

б) сведения о субъекте критической информационной инфраструктуры, которому на праве собственности, аренды или ином законном основании принадлежит объект критической информационной инфраструктуры;

в) сведения о взаимодействии объекта критической информационной инфраструктуры и сетей электросвязи;

г) сведения о лице, эксплуатирующем объект критической информационной инфраструктуры;

д) сведения о программных и программно-аппаратных средствах, используемых на объекте критической информационной инфраструктуры, в том числе средствах, используемых для обеспечения безопасности объекта критической информационной инфраструктуры и их сертификатах соответствия требованиям по безопасности информации (при наличии);

е) сведения об угрозах безопасности информации и о категориях нарушителей в отношении объекта критической информационной инфраструктуры либо об отсутствии таких угроз;

ж) возможные последствия в случае возникновения компьютерных инцидентов на объекте критической информационной инфраструктуры либо сведения об отсутствии таких последствий;

з) категорию значимости, которая присвоена объекту критической информационной инфраструктуры, или сведения об отсутствии необходимости присвоения одной из категорий значимости, а также сведения о результатах оценки показателей критериев значимости;

и) организационные и технические меры, применяемые для обеспечения безопасности объекта критической информационной инфраструктуры, либо сведения об отсутствии необходимости применения указанных мер.

18. Сведения, указанные в пункте 17 настоящих Правил, и их содержание направляются по форме, утверждаемой федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры.

19. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, проверяет сведения о результатах присвоения категорий значимости в порядке, предусмотренном частями 6 - 8 статьи 7 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации».

20. Категория значимости может быть изменена в порядке, предусмотренном для категорирования, в случаях, предусмотренных частью 12 статьи 7 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации».

21. Субъект критической информационной инфраструктуры не реже чем один раз в 5 лет осуществляет пересмотр установленной категории значимости в соответствии с настоящими Правилами. В случае изменения категории значимости сведения о результатах пересмотра категории значимости направляются в федеральный орган, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры.

Утвержден
постановлением Правительства
Российской Федерации
от 8 февраля 2018 г. N 127

ПЕРЕЧЕНЬ
ПОКАЗАТЕЛЕЙ КРИТЕРИЕВ ЗНАЧИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ И ИХ ЗНАЧЕНИЯ

	Показатель	Значение показателя		
		III категория	II категория	I категория
	I. Социальная значимость			
1.	Причинение ущерба жизни и здоровью людей (человек)	более или равно 1, но менее или равно 50	более 50, но менее или равно 500	более 500
2.	Прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения, в том числе объектов водоснабжения и канализации, очистки сточных вод, тепло- и электроснабжения, гидротехнических сооружений, оцениваемые:			
	а) на территории, на которой возможно нарушение обеспечения жизнедеятельности населения;	вся территория одного муниципального образования или одной внутригородской территории города федерального значения	выход за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта Российской Федерации или территории города федерального значения	выход за пределы территории одного субъекта Российской Федерации или территории города федерального значения
	б) по количеству людей, условия жизнедеятельности которых могут быть нарушены (тыс. человек)	более или равно 50, но менее 1000	более или равно 1000, но менее 5000	более или равно 5000
3.	Прекращение или нарушение функционирования объектов транспортной инфраструктуры, оцениваемые:			

	а) на территории, на которой возможно нарушение транспортного сообщения или предоставления транспортных услуг;	вся территория одного муниципального образования или одной внутригородской территории города федерального значения	выход за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта Российской Федерации или территории города федерального значения	выход за пределы территории одного субъекта Российской Федерации или территории города федерального значения
	б) по количеству людей, для которых могут быть недоступны транспортные услуги (тыс. человек)	более или равно 50, но менее 1000	более или равно 1000, но менее 5000	более или равно 5000
4.	Прекращение или нарушение функционирования сети связи, оцениваемые:			
	а) на территории, на которой возможно прекращение или нарушение функционирования сети связи;	вся территория одного муниципального образования или одной внутригородской территории города федерального значения	выход за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта Российской Федерации или территории города федерального значения	выход за пределы территории одного субъекта Российской Федерации или территории города федерального значения
	б) по количеству людей, для которых могут быть недоступны услуги связи (тыс. человек)	более или равно 50, но менее 1000	более или равно 1000, но менее 5000	более или равно 5000
5.	Отсутствие доступа к государственной услуге, оцениваемое в максимальном допустимом времени, в течение которого государственная услуга может быть недоступна для получателей такой услуги (часов)	менее или равно 24, но более 12	менее или равно 12, но более 6	менее 6

II. Политическая значимость

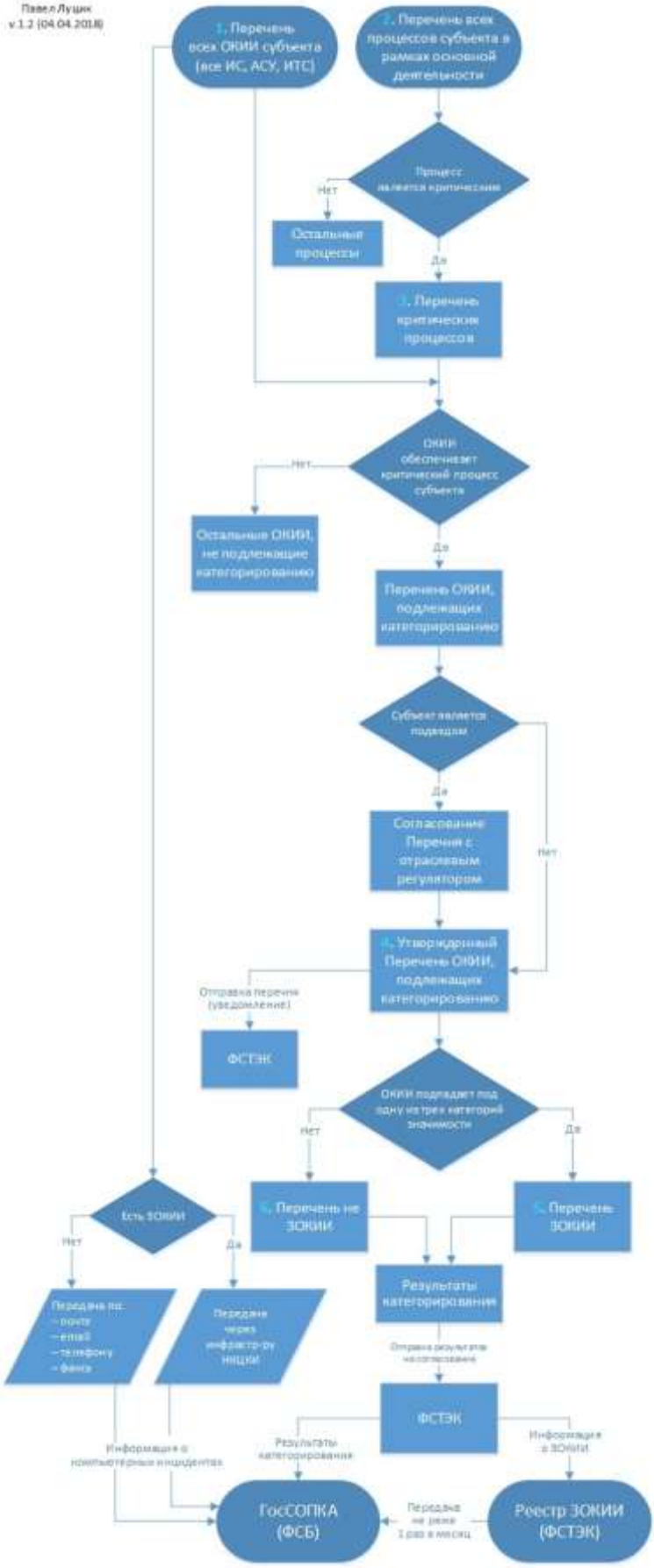
6.	Прекращение или нарушение функционирования государственного органа в части невыполнения возложенной на него функции (полномочия)	прекращение или нарушение функционирования органа государственной власти субъекта Российской Федерации или города федерального значения	прекращение или нарушение функционирования федерального органа государственной власти	прекращение или нарушение функционирования Администрации Президента Российской Федерации, Правительства Российской Федерации, Федерального Собрания Российской Федерации, Совета Безопасности Российской Федерации, Верховного Суда Российской Федерации, Конституционного Суда Российской Федерации
7.	Нарушение условий международного договора Российской Федерации, срыв переговоров или подписания планируемого к заключению международного договора Российской Федерации, оцениваемые по уровню международного договора Российской Федерации	нарушение условий договора межведомственного характера (срыв переговоров или подписания)	нарушение условий межправительственного договора (срыв переговоров или подписания)	нарушение условий межгосударственного договора (срыв переговоров или подписания)
	III. Экономическая значимость			
8.	Возникновение ущерба субъекту критической информационной инфраструктуры, который является государственной корпорацией, государственным унитарным предприятием, муниципальным унитарным предприятием, государственной компанией, организацией с участием государства и (или) стратегическим акционерным обществом, стратегическим предприятием, оцениваемого в снижении уровня дохода (с учетом налога на добавленную стоимость, акцизов и иных обязательных платежей) по всем видам деятельности (процентов прогнозируемого объема годового дохода по всем видам деятельности)	более 5, но менее или равно 10	более 10, но менее или равно 15	более 15
9.	Возникновение ущерба бюджетам Российской Федерации, оцениваемого:			
	а) в снижении доходов федерального бюджета, (процентов прогнозируемого годового дохода бюджета);	более 0,001, но менее или равно 0,05	более 0,005, но менее или равно 0,1	более 0,1

	б) в снижении доходов бюджета субъекта Российской Федерации (процентов прогнозируемого годового дохода бюджета);	более 0,001, но менее или равно 0,05	более 0,05, но менее или равно 0,1	более 0,1
	в) в снижении доходов бюджетов государственных внебюджетных фондов (процентов прогнозируемого годового дохода бюджета)	более 0,01, но менее или равно 0,5	более 0,5, но менее или равно 1	более 1
10.	Прекращение или нарушение проведения клиентами операций по банковским счетам и (или) без открытия банковского счета или операций, осуществляемых субъектом критической информационной инфраструктуры, являющимся в соответствии с законодательством Российской Федерации системно значимой кредитной организацией, оператором услуг платежной инфраструктуры системно и (или) социально значимых платежных систем или системно значимой инфраструктурной организацией финансового рынка, оцениваемое среднедневным (по отношению к числу календарных дней в году) количеством осуществляемых операций, (млн. единиц) (расчет осуществляется по итогам года, а для создаваемых объектов - на основе прогнозных значений)	более 3, но менее или равно 70	более 70, но менее или равно 120	более 120
	IV. Экологическая значимость			
11.	Вредные воздействия на окружающую среду (ухудшение качества воды в поверхностных водоемах, обусловленное сбросами загрязняющих веществ, повышение уровня вредных загрязняющих веществ, в том числе радиоактивных веществ, в атмосферу, ухудшение состояния земель в результате выбросов или сбросов загрязняющих веществ или иные вредные воздействия), оцениваемые:			

	а) на территории, на которой окружающая среда может подвергнуться вредным воздействиям;	вся территория одного муниципального образования или одной внутригородской территории города федерального значения	выход за пределы территории одного муниципального образования или одной внутригородской территории города федерального значения, но не за пределы территории одного субъекта Российской Федерации или территории города федерального значения	выход за пределы территории одного субъекта Российской Федерации или территории города федерального значения
	б) по количеству людей, которые могут быть подвержены вредным воздействиям (тыс. человек)	более или равно 50, но менее 1000	более или равно 1000, но менее 5000	более или равно 5000
	V. Значимость для обеспечения обороны страны, безопасности государства и правопорядка			
12.	Прекращение или нарушение (невыполнение установленных показателей) функционирования пункта управления (ситуационного центра), оцениваемое в уровне (значимости) пункта управления или ситуационного центра	прекращение или нарушение функционирования пункта управления или ситуационного центра органа государственной власти субъекта Российской Федерации или города федерального значения	прекращение или нарушение функционирования пункта управления или ситуационного центра федерального органа государственной власти или государственной корпорации	прекращение или нарушение функционирования пункта управления государством или ситуационного центра Администрации Президента Российской Федерации, Правительства Российской Федерации, Федерального Собрания Российской Федерации, Совета Безопасности Российской Федерации, Верховного Суда Российской Федерации, Конституционного Суда Российской Федерации
13.	Снижение показателей государственного оборонного заказа, выполняемого субъектом критической информационной инфраструктуры, оцениваемое:			

	а) в снижении объемов продукции (работ, услуг) в заданный период времени (процентов заданного объема продукции);	более 5, но менее или равно 10	более 10, но менее или равно 15	более 15
	б) в увеличении времени выпуска продукции (работ, услуг) с заданным объемом (процентов установленного времени выпуска продукции)	более 3, но менее или равно 10	более 10, но менее или равно 40	более 40
14.	Прекращение или нарушение функционирования (невыполнения установленных показателей) информационной системы в области обеспечения обороны страны, безопасности государства и правопорядка, оцениваемое в максимально допустимом времени, в течение которого информационная система может быть недоступна пользователю (часов)	менее или равно 4, но более 2	менее или равно 2, но более 1	более 1

Весь процесс категорирования объектов КИИ и передачи информации во ФСТЭК и в ГосСОПКА - на одной схеме



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ

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

от 24 августа 2018 г. № 240/25/3752

С 1 января 2018 г. вступил в силу Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

В соответствии со статьей 7 указанного Федерального закона и постановлением Правительства Российской Федерации от 8 февраля 2018 г. № 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» субъекты критической информационной инфраструктуры осуществляют категорирование объектов критической информационной инфраструктуры Российской Федерации, в ходе которого формируют и направляют в ФСТЭК России перечни объектов критической информационной инфраструктуры, подлежащих категорированию.

Для единообразного подхода к формированию перечней объектов критической информационной инфраструктуры, подлежащих категорированию, рекомендуется:

1. Направлять в ФСТЭК России утвержденный руководителем субъекта критической информационной инфраструктуры (или уполномоченным лицом) перечень объектов критической информационной инфраструктуры, подлежащих категорированию, оформленный в соответствии с приложением 1.

2. Прикладывать при направлении в ФСТЭК России электронную копию перечня объектов критической информационной инфраструктуры, подлежащих категорированию, для сокращения срока оценки перечня (формат docx, xlsx).

3. Прикладывать при представлении в ФСТЭК России электронную копию сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий для удобства формирования и ведения Реестра значимых объектов критической информационной инфраструктуры Российской Федерации (формат docx, xlsx).

Одновременно отмечаем, что предоставление информации об отсутствии в организации объектов критической информационной инфраструктуры или о том, что организация не является субъектом критической информационной инфраструктуры Российской Федерации в ФСТЭК России в соответствии с законодательством о безопасности критической информационной инфраструктуры Российской Федерации не требуется.

Заместитель директора
ФСТЭК России В.Лютиков

Приложение 1
к информационному сообщению ФСТЭК России
от 24 августа 2018 г. № 240/25/3752

Рекомендуемая форма перечня объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

УТВЕРЖДАЮ

_____

Должность руководителя субъекта критической информационной инфраструктуры Российской Федерации (далее – субъект) или уполномоченного им лица

_____ _____

Подпись руководителя субъекта или уполномоченного им лица

Фамилия, имя, отчество (при наличии) руководителя субъекта или уполномоченного им лица

« ___ » _____ 20___ г.

Дата утверждения перечня объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

Перечень объектов критической информационной инфраструктуры Российской Федерации, подлежащих категорированию

№ п/п	Наименование объекта	Тип объекта[1]	Сфера (область) деятельности, в которой функционирует объект [2]	Планируемый срок категорирования объекта	Должность, фамилия, имя, отчество (при наличии) представителя, его телефон, адрес электронной почты (при наличии)[3]
1.					
2.					
…					
n.					

[1] Указывается один из следующих типов объекта: информационная система, автоматизированная система управления, информационно-телекоммуникационная сеть.

[2] Указывается сфера (область) в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации инфраструктуры Российской Федерации».

[3] Указываются должность, фамилия, имя, отчество (при наличии) должностного лица, с которым можно осуществить взаимодействие по вопросам категорирования объекта, его телефон, адрес электронной почты (при наличии). Для нескольких объектов может быть определено одно должностное лицо.

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ
ПОСТАНОВЛЕНИЕ

от 17 февраля 2018 г. N 162

ОБ УТВЕРЖДЕНИИ ПРАВИЛ ОСУЩЕСТВЛЕНИЯ ГОСУДАРСТВЕННОГО КОНТРОЛЯ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

В соответствии с пунктом 2 части 2 статьи 6 Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» Правительство Российской Федерации постановляет:

Утвердить прилагаемые Правила осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации.

Председатель Правительства
Российской Федерации Д.МЕДВЕДЕВ

Утверждены
постановлением Правительства
Российской Федерации
от 17 февраля 2018 г. N 162

ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ГОСУДАРСТВЕННОГО КОНТРОЛЯ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

I. Общие положения

1. Настоящие Правила устанавливают порядок осуществления федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, и его территориальными органами (далее - орган государственного контроля) мероприятий по государственному контролю в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (далее соответственно - критическая информационная инфраструктура, государственный контроль).

2. Государственный контроль проводится в целях проверки соблюдения субъектами критической информационной инфраструктуры, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, требований, установленных Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации» и принятыми в соответствии с ним нормативными правовыми актами (далее соответственно - требования по обеспечению безопасности, проверка).

3. Государственный контроль осуществляется путем проведения плановых и внеплановых выездных проверок.

4. Для осуществления проверки органом государственного контроля создается комиссия в составе не менее 2 должностных лиц. Внеплановая проверка, проводимая по основанию, указанному в подпункте «а» пункта 20 настоящих Правил, может осуществляться одним должностным лицом органа государственного контроля.

5. Проверка проводится должностными лицами органа государственного контроля, которые указаны в приказе органа государственного контроля о проведении проверки.

6. Срок проведения плановой проверки не должен превышать 20 рабочих дней.

7. Срок проведения внеплановой проверки не должен превышать 10 рабочих дней.

8. Срок проведения каждой из проверок, предусмотренных пунктом 3 настоящих Правил, в отношении субъекта критической информационной инфраструктуры, который осуществляет свою деятельность на территориях нескольких субъектов Российской Федерации, устанавливается отдельно по каждому филиалу, представительству и обособленному структурному подразделению субъекта критической информационной инфраструктуры, при этом общий срок проведения проверки не может превышать 60 рабочих дней.

9. Проверки в отношении значимых объектов критической информационной инфраструктуры, которые на праве собственности, аренды или ином законном основании принадлежат Министерству обороны Российской Федерации, Службе внешней разведки Российской Федерации, Федеральной службе безопасности Российской Федерации, Федеральной службе охраны Российской Федерации и Главному управлению специальных программ Президента Российской Федерации, а также значимых объектов критической информационной инфраструктуры, защита которых входит в их компетенцию, проводятся по согласованию с руководителями указанных федеральных органов исполнительной власти.

10. Информация об организации проверок, в том числе об их планировании, о проведении и результатах таких проверок, в органы прокуратуры не направляется, за исключением

информации о результатах проверок, проведенных на основании требования прокурора об осуществлении внеплановой проверки в рамках проведения надзора за исполнением законов по поступившим в органы прокуратуры материалам и обращениям.

II. Организация плановой проверки

11. Предметом плановой проверки является соблюдение субъектом критической информационной инфраструктуры требований по обеспечению безопасности.

12. Основаниями для осуществления плановой проверки являются истечение 3 лет со дня:

а) внесения сведений об объекте критической информационной инфраструктуры в реестр значимых объектов критической информационной инфраструктуры;

б) окончания осуществления последней плановой проверки в отношении значимого объекта критической информационной инфраструктуры.

13. Ежегодный план проведения плановых проверок утверждается руководителем органа государственного контроля до 20 декабря года, предшествующего году проведения плановых проверок.

14. Ежегодный план проведения плановых проверок содержит следующую информацию:

а) сведения о субъекте критической информационной инфраструктуры;

б) сведения о лице, эксплуатирующем значимый объект критической информационной инфраструктуры;

в) дату окончания последней плановой проверки;

г) месяц и срок проведения проверки;

д) основание проведения проверки;

е) наименование органа государственного контроля.

15. Выписки из утвержденного ежегодного плана проведения плановых проверок направляются до 1 января года проведения плановых проверок органом государственного контроля субъектам критической информационной инфраструктуры.

16. О проведении плановой проверки субъект критической информационной инфраструктуры уведомляется органом государственного контроля не менее чем за 3 рабочих дня до начала ее проведения посредством направления копии приказа органа государственного контроля о проведении плановой проверки любым доступным способом, обеспечивающим возможность подтверждения факта такого уведомления.

17. Плановая проверка проводится на основании утвержденного ежегодного плана проведения плановых проверок и приказа органа государственного контроля о проведении проверки.

18. В приказе органа государственного контроля о проведении проверки указываются:

а) наименование органа государственного контроля, номер и дата издания приказа;

б) должности, фамилии, имена и отчества должностных лиц органа государственного контроля, уполномоченных на проведение проверки;

в) сведения о субъекте критической информационной инфраструктуры;

г) сведения о лице, эксплуатирующем значимый объект критической информационной инфраструктуры;

д) задачи проверки;

е) дата начала и окончания проверки;

ж) срок проведения проверки;

з) правовые основания проведения проверки, в том числе нормативные правовые акты, соблюдение положений которых подлежит проверке;

и) перечень мероприятий по контролю, необходимых для выполнения задач проверки.

III. Организация внеплановой проверки

19. Предметом внеплановой проверки является соблюдение субъектом критической информационной инфраструктуры требований по обеспечению безопасности, выполнение предписания органа государственного контроля, а также проведение мероприятий по предотвращению негативных последствий на значимом объекте критической информационной инфраструктуры, причиной которых является возникновение компьютерного инцидента.

20. Основаниями для осуществления внеплановой проверки являются:

а) истечение срока выполнения субъектом критической информационной инфраструктуры выданного органом государственного контроля предписания об устранении выявленного нарушения требований по обеспечению безопасности;

б) возникновение компьютерного инцидента на значимом объекте критической информационной инфраструктуры, повлекшего негативные последствия;

в) приказ органа государственного контроля, изданный в соответствии с поручением Президента Российской Федерации или Правительства Российской Федерации либо на основании требования прокурора об осуществлении внеплановой проверки в рамках проведения надзора за исполнением законов по поступившим в органы прокуратуры материалам и обращениям.

21. О проведении внеплановой проверки (за исключением внеплановой проверки, основание для осуществления которой указано в подпункте «б» пункта 20 настоящих Правил) субъект критической информационной инфраструктуры уведомляется органом государственного контроля не менее чем за 24 часа до начала ее проведения любым доступным способом, обеспечивающим возможность подтверждения факта такого уведомления.

22. В случае если внеплановая проверка проводится по основанию, указанному в подпункте «б» пункта 20 настоящих Правил, орган государственного контроля вправе приступить к проведению внеплановой проверки незамедлительно.

23. Внеплановая проверка проводится на основании приказа органа государственного контроля о проведении проверки, оформленного в соответствии с пунктом 18 настоящих Правил.

IV. Проведение проверки

24. Плановая и внеплановая проверка проводится по месту нахождения субъекта критической информационной инфраструктуры, лица, эксплуатирующего значимый объект критической информационной инфраструктуры, и значимого объекта критической информационной инфраструктуры.

25. Проверка начинается с предъявления служебного удостоверения должностными лицами органа государственного контроля, обязательного ознакомления руководителя субъекта критической информационной инфраструктуры или уполномоченного им должностного лица с приказом органа государственного контроля о проведении проверки.

26. Руководителю субъекта критической информационной инфраструктуры или уполномоченному им должностному лицу под расписку передается копия приказа органа государственного контроля о проведении проверки, заверенная печатью органа государственного контроля.

27. Руководитель субъекта критической информационной инфраструктуры или уполномоченное им должностное лицо обязаны предоставить должностным лицам органа государственного контроля, осуществляющим проверку, возможность ознакомиться с документами, связанными с предметом и задачами проверки, а также обеспечить с учетом требований пропускного режима беспрепятственный доступ проводящих проверку должностных лиц на территорию, в используемые при осуществлении деятельности здания, строения, сооружения, помещения и к значимым объектам критической информационной инфраструктуры.

28. Для оценки эффективности принимаемых мер во исполнение требований по обеспечению безопасности должностными лицами органа государственного контроля используются сертифицированные по требованиям безопасности информации программные и аппаратно-программные средства контроля, в том числе имеющиеся у субъекта критической информационной инфраструктуры.

Возможность и порядок использования таких средств контроля с учетом особенностей функционирования значимого объекта критической информационной инфраструктуры согласовывается с руководителем субъекта критической информационной инфраструктуры или уполномоченным им должностным лицом.

V. Ограничения при проведении проверки

29. При проведении проверки должностные лица органа государственного контроля не вправе:

а) проверять выполнение требований по обеспечению безопасности, если они не относятся к полномочиям органа государственного контроля, от имени которого действуют эти должностные лица;

б) проводить проверку в случае отсутствия при ее проведении руководителя субъекта критической информационной инфраструктуры или уполномоченного им должностного лица, за исключением случая проведения проверки по основанию, указанному в подпункте «б» пункта 20 настоящих Правил;

в) требовать представления документов и информации, если они не относятся к предмету проверки, а также изымать оригиналы таких документов;

г) распространять информацию, полученную в результате проведения проверки и составляющую государственную, коммерческую, служебную и иную охраняемую законом тайну, за исключением случаев, предусмотренных законодательством Российской Федерации;

д) превышать установленные сроки проведения проверки;

е) осуществлять выдачу субъектам критической информационной инфраструктуры предписаний или предложений о проведении за их счет мероприятий по контролю;

ж) осуществлять действия с техническими средствами обработки информации, в результате которых может быть нарушено и (или) прекращено функционирование значимого объекта критической информационной инфраструктуры.

VI. Обязанности должностных лиц органа государственного контроля при проведении проверки

30. Должностные лица органа государственного контроля при проведении проверки обязаны:

а) своевременно и в полной мере исполнять предоставленные в соответствии с законодательством Российской Федерации полномочия по предупреждению, выявлению и пресечению нарушений субъектом критической информационной инфраструктуры требований по обеспечению безопасности;

б) соблюдать права и законные интересы субъекта критической информационной инфраструктуры, проверка которого проводится;

в) проводить проверку на основании приказа органа государственного контроля о ее проведении в соответствии с ее предметом и задачами;

г) проводить проверку во время исполнения служебных обязанностей и при предъявлении служебных удостоверений и копии приказа органа государственного контроля о проведении проверки;

д) не препятствовать руководителю субъекта критической информационной инфраструктуры или уполномоченному им должностному лицу присутствовать при проведении проверки и давать разъяснения по вопросам, относящимся к предмету проверки;

е) предоставлять руководителю субъекта критической информационной инфраструктуры или уполномоченному им должностному лицу, присутствующим при проведении проверки, информацию и документы, относящиеся к предмету проверки;

ж) знакомить руководителя субъекта критической информационной инфраструктуры или уполномоченное им должностное лицо с результатами проверки;

з) соблюдать сроки проведения проверки, установленные настоящими Правилами;

и) не требовать от субъекта критической информационной инфраструктуры документы и иные сведения, представление которых не предусмотрено законодательством Российской Федерации;

к) в случае, предусмотренном внутренним распорядком субъекта критической информационной инфраструктуры, пройти в первый день проверки инструктаж по соблюдению техники безопасности при нахождении на территории, на которой расположен проверяемый значимый объект критической информационной инфраструктуры;

л) осуществлять запись о проведенной проверке в журнале учета проверок при его наличии.

VII. Порядок оформления результатов проверки

31. По результатам проверки должностными лицами органа государственного контроля, проводящими проверку, составляется акт проверки.

32. Форма акта проверки утверждается федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры.

33. В акте проверки указываются:

а) дата и место составления акта проверки;

б) наименование органа государственного контроля;

в) дата и номер приказа органа государственного контроля о проведении проверки;

г) продолжительность и место проведения проверки;

д) фамилии, имена, отчества и должности лиц, проводивших проверку;

е) сведения о субъекте критической информационной инфраструктуры;

ж) фамилия, имя и отчество руководителя субъекта критической информационной инфраструктуры или уполномоченного им должностного лица, присутствовавших при проведении проверки;

з) сведения о лице, эксплуатирующем значимый объект критической информационной инфраструктуры;

и) сведения о проверяемом значимом объекте критической информационной инфраструктуры;

к) сведения о результатах проверки, в том числе о выявленных нарушениях требований по обеспечению безопасности;

л) сведения о внесении в журнал учета проверок записи о проведенной проверке либо о невозможности внесения такой записи в связи с отсутствием у субъекта критической информационной инфраструктуры указанного журнала;

м) подписи должностных лиц органа государственного контроля, проводивших проверку;

н) сведения об ознакомлении или отказе от ознакомления с актом проверки руководителя субъекта критической информационной инфраструктуры или уполномоченного им должностного лица.

34. На основании акта проверки в случае выявления нарушения требований по обеспечению безопасности орган государственного контроля выдает субъекту критической информационной инфраструктуры предписание об устранении выявленного нарушения с указанием срока его устранения.

35. К акту проверки прилагаются протоколы или заключения по результатам контрольных мероприятий, проведенных с использованием программных и аппаратно-программных средств

контроля, а также предписания об устранении выявленных нарушений и иные связанные с результатами проверки документы или их копии.

36. Акт проверки оформляется непосредственно после ее завершения в 3 экземплярах, один из которых с приложениями вручается руководителю субъекта критической информационной инфраструктуры или уполномоченному им должностному лицу. Второй экземпляр акта проверки направляется в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры, третий - в территориальный орган федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры, проводивший проверку.

37. В случае проведения внеплановой проверки на основании требования прокурора об осуществлении внеплановой проверки в рамках проведения надзора за исполнением законов по поступившим в органы прокуратуры материалам и обращениям копия акта проверки с копиями приложений высылается в соответствующий орган прокуратуры.

38. Результаты проверки, содержащие информацию, составляющую государственную, коммерческую, служебную и иную охраняемую законом тайну, оформляются с соблюдением требований, предусмотренных законодательством Российской Федерации.

VIII. Меры, принимаемые должностными лицами органа государственного контроля в отношении фактов нарушения требований по обеспечению безопасности, выявленных при проведении проверки

39. В случае выявления при проведении проверки нарушения субъектом критической информационной инфраструктуры требований по обеспечению безопасности должностные лица органа государственного контроля, проводившие проверку, в пределах полномочий, предусмотренных законодательством Российской Федерации, обязаны:

а) выдать предписание субъекту критической информационной инфраструктуры об устранении выявленного нарушения требований по обеспечению безопасности с указанием срока его устранения, который устанавливается в том числе с учетом утвержденных и представленных субъектом критической информационной инфраструктуры программ (планов) по модернизации (дооснащению) значимого объекта критической информационной инфраструктуры;

б) принять меры по контролю за устранением выявленного нарушения, его предупреждению и предотвращению.

40. В случае невозможности выполнения предписания, предусмотренного подпунктом «а» пункта 39 настоящих Правил, по причинам, не зависящим от субъекта критической информационной инфраструктуры, руководитель органа государственного контроля при поступлении в орган государственного контроля мотивированного обращения субъекта критической информационной инфраструктуры вправе продлить срок выполнения указанного предписания, но не более чем на один год, уведомив об этом субъекта критической информационной инфраструктуры в течение 30 дней со дня регистрации указанного обращения.

IX. Ответственность органа государственного контроля и его должностных лиц при проведении проверки

41. Орган государственного контроля и его должностные лица в случае ненадлежащего исполнения соответственно функций, служебных обязанностей и совершения противоправных действий (бездействия) при проведении проверки несут ответственность в соответствии с законодательством Российской Федерации.

42. Орган государственного контроля осуществляет контроль за исполнением должностными лицами органа государственного контроля служебных обязанностей, ведет учет случаев ненадлежащего исполнения должностными лицами служебных обязанностей, проводит соответствующие служебные проверки и принимает в соответствии с законодательством Российской Федерации меры в отношении таких должностных лиц.

43. Орган государственного контроля обязан сообщить в письменной форме субъекту критической информационной инфраструктуры, права и (или) законные интересы которого нарушены, о мерах, принятых в отношении виновных в нарушении законодательства Российской Федерации должностных лиц, в течение 10 дней со дня принятия таких мер.

X. Недействительность результатов проверки, проведенной с грубым нарушением положений настоящих Правил

44. Результаты проверки, проведенной органом государственного контроля с грубым нарушением положений настоящих Правил, не могут являться доказательствами нарушения субъектом критической информационной инфраструктуры требований по обеспечению безопасности и подлежат отмене органом государственного контроля на основании заявления субъекта критической информационной инфраструктуры.

45. К грубым нарушениям положений настоящих Правил относятся:

а) отсутствие оснований для проведения проверки;

б) нарушение срока уведомления о проведении проверки;

в) нарушение срока проведения проверки;

г) проведение проверки без приказа органа государственного контроля;

д) невручение руководителю субъекта критической информационной инфраструктуры или уполномоченному им должностному лицу акта проверки;

е) проведение плановой проверки, не включенной в ежегодный план проведения плановых проверок.

XI. Права, обязанности и ответственность субъекта критической информационной инфраструктуры при осуществлении государственного контроля

46. Руководитель субъекта критической информационной инфраструктуры или уполномоченное им должностное лицо при проведении проверки имеют право:

а) получать от органа государственного контроля и его должностных лиц информацию, которая относится к предмету проверки и представление которой предусмотрено настоящими Правилами;

б) знакомиться с результатами проверки и указывать в акте проверки о своем ознакомлении с результатами проверки, согласии или несогласии с ними, а также с отдельными действиями должностных лиц органа государственного контроля;

в) обжаловать действия (бездействие) должностных лиц органа государственного контроля, повлекшие за собой нарушение прав субъекта критической информационной инфраструктуры при проведении проверки, в административном и (или) судебном порядке в соответствии с законодательством Российской Федерации.

47. Руководитель субъекта критической информационной инфраструктуры или уполномоченное им должностное лицо при проведении проверки обязаны:

а) непосредственно присутствовать при проведении проверки и давать пояснения по вопросам, относящимся к предмету проверки;

б) предоставить должностным лицам органа государственного контроля, проводящим проверку, возможность ознакомиться с документами, связанными с задачами и предметом проверки;

в) выполнять предписания должностных лиц органа государственного контроля об устранении нарушений в части соблюдения требований по обеспечению безопасности, выданные этими лицами в соответствии со своей компетенцией;

г) обеспечить с учетом требований пропускного режима беспрепятственный доступ проводящих проверку должностных лиц на территорию, в используемые при осуществлении деятельности здания, строения, сооружения, помещения и к значимым объектам критической информационной инфраструктуры;

д) в случае, предусмотренном внутренним распорядком субъекта критической информационной инфраструктуры, провести в первый день проверки инструктаж по соблюдению техники безопасности при нахождении на территории, на которой расположен проверяемый значимый объект критической информационной инфраструктуры, с должностными лицами органа государственного контроля, осуществляющими проверку;

е) принимать меры по устранению выявленных нарушений.

48. Руководитель субъекта критической информационной инфраструктуры или уполномоченное им должностное лицо, допустившие нарушение положений настоящих Правил, необоснованно препятствующие проведению проверки, уклоняющиеся от проведения проверки и (или) не выполняющие в установленный срок предписания органа государственного контроля об устранении выявленных нарушений требований по обеспечению безопасности, несут ответственность в соответствии с законодательством Российской Федерации.

49. В случае невозможности выполнения предписания, предусмотренного подпунктом «а» пункта 39 настоящих Правил, по причинам, не зависящим от субъекта критической информационной инфраструктуры, субъект критической информационной инфраструктуры до истечения срока выполнения предписания вправе обратиться с мотивированным обращением о продлении срока выполнения предписания к руководителю органа государственного контроля, выдавшему такое предписание. Обращение субъекта критической информационной инфраструктуры подлежит рассмотрению в порядке, предусмотренном пунктом 40 настоящих Правил.

50. В случае несогласия с фактами, изложенными в акте проверки и (или) предписании об устранении выявленного нарушения, руководитель субъекта критической информационной инфраструктуры или уполномоченное им должностное лицо вправе представить в течение 15 дней с даты получения акта проверки в проводивший проверку орган государственного контроля возражения в письменной форме в отношении акта проверки и (или) выданного предписания об устранении выявленного нарушения в целом или их отдельных положений. При этом субъект критической информационной инфраструктуры вправе приложить к возражениям документы, подтверждающие обоснованность таких возражений, или их заверенные копии либо в согласованный срок передать их в орган государственного контроля.

Зарегистрировано в Минюсте России 8 февраля 2018 г. N 49966

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ПРИКАЗ
от 6 декабря 2017 г. N 227

ОБ УТВЕРЖДЕНИИ ПОРЯДКА ВЕДЕНИЯ РЕЕСТРА ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

В соответствии с пунктом 2 части 3 статьи 6 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" (Собрание законодательства Российской Федерации, 2017, N 31, ст. 4736) приказываю:

Утвердить прилагаемый Порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации.

Директор Федеральной службы
по техническому и экспортному контролю В.СЕЛИН

Утвержден
приказом ФСТЭК России
от 6 декабря 2017 г. N 227

ПОРЯДОК
ВЕДЕНИЯ РЕЕСТРА ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

1. Настоящий Порядок определяет правила формирования и ведения Реестра значимых объектов критической информационной инфраструктуры Российской Федерации (далее - Реестр) с целью учета значимых объектов критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура) в ходе межотраслевой координации деятельности по обеспечению значимых объектов критической информационной инфраструктуры, осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, а также проведения иных мероприятий в области обеспечения безопасности критической информационной инфраструктуры в соответствии с Федеральным законом от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" (далее - Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации").

2. Ведение Реестра осуществляется в целях учета, хранения и предоставления информации в бумажном и электронном виде о значимых объектах критической информационной инфраструктуры, принадлежащих на праве собственности, аренды или ином законном основании субъектам критической информационной инфраструктуры <*>.

<*> *Пункт 8 статьи 2 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".*

3. Реестр формируется и ведется Федеральной службой по техническому и экспортному контролю на основе сведений, представляемых субъектами критической информационной инфраструктуры в соответствии с частью 5 статьи 7 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" (далее - сведения об объектах критической информационной инфраструктуры).

Субъекты критической информационной инфраструктуры должны обеспечивать достоверность и актуальность представляемых сведений об объектах критической информационной инфраструктуры.

4. Решение о включении сведений о значимом объекте критической информационной инфраструктуры в Реестр принимается в течение 30 дней со дня получения ФСТЭК России сведений от субъекта критической информационной инфраструктуры.

5. В соответствии с частью 1 статьи 8 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" в Реестр вносятся следующие сведения о значимом объекте критической информационной инфраструктуры:

а) наименование значимого объекта критической информационной инфраструктуры;

б) наименование субъекта критической информационной инфраструктуры;

в) сведения о взаимодействии значимого объекта критической информационной инфраструктуры и сетей электросвязи;

г) сведения о лице, эксплуатирующем значимый объект критической информационной инфраструктуры;

д) категория значимости, которая присвоена объекту критической информационной инфраструктуры субъектом критической информационной инфраструктуры;

е) сведения о программных и программно-аппаратных средствах, используемых на значимом объекте критической информационной инфраструктуры;

ж) меры, применяемые для обеспечения безопасности значимого объекта критической информационной инфраструктуры.

6. Каждому значимому объекту критической информационной инфраструктуры, включенному в Реестр, присваивается регистрационный номер, состоящий из групп цифр и прописных букв, разделенных косыми чертами, который имеет вид: XXXXXX/X/XX/X.

Первая группа знаков содержит число от 000001 до 999999, указывающее на порядковый номер значимого объекта критической информационной инфраструктуры в Реестре.

Вторая группа знаков содержит число, обозначающее федеральный округ, на территории которого находится значимый объект критической информационной инфраструктуры:

1 - Центральный федеральный округ;

2 - Северо-Западный федеральный округ;

3 - Южный федеральный округ;

4 - Северо-Кавказский федеральный округ;

5 - Приволжский федеральный округ;

6 - Уральский федеральный округ;

7 - Сибирский федеральный округ;

8 - Дальневосточный федеральный округ.

Третья группа знаков содержит двузначное число, обозначающее сферу (область) деятельности, в которой функционирует значимый объект критической информационной инфраструктуры, определенную в соответствии с пунктом 8 статьи 2 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации":

1 - здравоохранение;

2 - наука;

3 - транспорт;

4 - связь;

5 - банковская сфера и иные сферы финансового рынка;

6 - энергетика и топливно-энергетический комплекс;

7 - атомная энергия;

8 - оборонная промышленность;

9 - ракетно-космическая промышленность;

10 - горнодобывающая промышленность;

11 - металлургическая промышленность;

12 - химическая промышленность.

Четвертая группа знаков содержит прописную букву, которая обозначает тип значимого объекта критической информационной инфраструктуры:

"А" - информационная система;

"Б" - автоматизированная система управления технологическими (производственными) процессами;

"В" - информационно-телекоммуникационная сеть.

В случае если значимый объект критической информационной инфраструктуры функционирует в нескольких сферах (областях) деятельности или расположен на территории нескольких федеральных округов, второй и третьей группам цифр присваивается обозначение сферы (области) деятельности или территории, указанные субъектом критической информационной инфраструктуры первыми. Обозначение других сфер (областей) деятельности, в которых функционирует значимый объект критической информационной инфраструктуры, или территорий федеральных округов, на которых он располагается, вносится в графу Реестра, содержащую дополнительные сведения о значимом объекте критической информационной инфраструктуры.

7. Записи о значимых объектах критической информационной инфраструктуры в Реестре ведутся последовательно в соответствии с датой включения в него сведений о значимом объекте критической информационной инфраструктуры.

8. В случае изменения сведений о значимых объектах критической информационной инфраструктуры субъекты критической информационной инфраструктуры должны направить измененные сведения в ФСТЭК России.

Изменения в Реестр вносятся только на основе сведений, представляемых субъектами критической информационной инфраструктуры.

9. В случае внесения изменений в сведения о значимом объекте критической информационной инфраструктуры регистрационный номер значимого объекта критической информационной инфраструктуры, включенного в Реестр, не изменяется.

10. В случае изменения значимого объекта критической информационной инфраструктуры, в результате которого такой объект перестал соответствовать критериям значимости и показателям их значений, и ему не может быть присвоена ни одна из категорий значимости, субъект критической информационной инфраструктуры должен направить об этом сведения в ФСТЭК России.

На основании сведений, представленных субъектом критической информационной инфраструктуры, объект критической информационной инфраструктуры исключается из Реестра.

11. В случае исключения значимого объекта критической информационной инфраструктуры из Реестра ранее присвоенный такому объекту регистрационный номер в дальнейшем не используется.

12. Сведения из Реестра не реже чем один раз в месяц направляются в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации в соответствии со статьей 5 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации".

Сведения из Реестра могут предоставляться государственным органам или российским юридическим лицам, выполняющим функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере, указанным в части 2 статьи 11 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" по их запросам только в части значимых объектов критической информационной инфраструктуры, функционирующих в сферах, отнесенных в компетенции этих государственных органов или российских юридических лиц.

13. В ходе формирования и ведения Реестра ФСТЭК России должны быть обеспечены:

безопасность информации ограниченного доступа, содержащейся в Реестре, в соответствии с законодательством Российской Федерации о государственной тайне;

поддержание содержащихся в Реестре сведений о значимых объектах критической информационной инфраструктуры в актуальном состоянии в соответствии с представленными субъектами критической информационной инфраструктуры сведениями;

использование содержащихся в Реестре сведений о значимых объектах критической информационной инфраструктуры только в рамках предоставленных ФСТЭК России полномочий в области обеспечения безопасности критической информационной инфраструктуры;

полнота и актуальность сведений о значимых объектах критической информационной инфраструктуры, предоставляемых в соответствии с пунктом 12 настоящего Порядка;

информирование субъектов критической информационной инфраструктуры о внесении в Реестр сведений о значимых объектах критической информационной инфраструктуры в сроки, установленные частью 7 статьи 7 Федерального закона "О безопасности критической информационной инфраструктуры", с указанием дат внесения сведений в Реестр и присвоенных регистрационных номеров.

14. В целях сохранности сведений о значимых объектах критической информационной инфраструктуры, включенных в Реестр, ФСТЭК России обеспечивается резервирование Реестра. Резервная копия Реестра формируется не реже одного раза в месяц путем записи на учтенные съемные машинные носители информации. Срок хранения машинных носителей информации составляет не менее 5 лет.

Зарегистрировано в Минюсте России 28 декабря 2017 г. N 49500

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ПРИКАЗ
от 11 декабря 2017 г. N 229

ОБ УТВЕРЖДЕНИИ ФОРМЫ АКТА ПРОВЕРКИ, СОСТАВЛЯЕМОГО ПО ИТОГАМ ПРОВЕДЕНИЯ ГОСУДАРСТВЕННОГО КОНТРОЛЯ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

В соответствии с пунктом 5 части 3 статьи 6 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" (Собрание законодательства Российской Федерации, 2017, N 31, ст. 4736) приказываю:

Утвердить прилагаемую форму акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации.

Директор Федеральной службы
по техническому и экспортному контролю В.СЕЛИН

Приложение
к приказу ФСТЭК России
от 11 декабря 2017 г. N 229

Форма

Гриф секретности
или
ограничительная пометка
Экз. N __

_____
(наименование органа государственного контроля)

АКТ ПРОВЕРКИ
по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

"__" _____ 20__ г. _____
(дата составления акта проверки) (место составления акта проверки)

На основании _____
(дата и номер приказа органа государственного контроля)

в период с "__" _____ 20__ г. по "__" _____ 20__ г. была проведена _____
(плановая/внеплановая)

выездная проверка общей продолжительностью _____ рабочих дней в отношении _____
(наименование субъекта критической информационной инфраструктуры)

и принадлежащего (принадлежащих) ему значимого объекта (значимых объектов) критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура) _____
_____.
(наименование и категория значимости значимого объекта критической информационной инфраструктуры)

Эксплуатацию значимого объекта (значимых объектов) критической информационной инфраструктуры осуществляет: _____
_____.
(наименование лица, эксплуатирующего значимый объект критической информационной инфраструктуры)

Место проведения проверки: _____.

Должностное лицо (должностные лица) органа государственного контроля, проводившее (проводившие) проверку: _____.
(фамилия, имя, отчество (последнее - при наличии) и должность)

С копией приказа о проведении проверки ознакомлен _____
_____.
(фамилия, инициалы, подпись, дата)

При проведении проверки присутствовал: _____
(фамилия, имя, отчество (последнее - при наличии)
_____.
и должность руководителя субъекта критической информационной инфраструктуры (его филиала, представительства или обособленного структурного подразделения) или уполномоченного им должностного лица)

В ходе проведения проверки установлено:
_____;
(указываются сведения о выполнении субъектом критической информационной

инфраструктуры требований, установленных Федеральным законом "О безопасности критической информационной инфраструктуры Российской Федерации" и принятыми в соответствии с ним нормативными правовыми актами (далее - требования по обеспечению безопасности)

_____.

(указываются сведения о результатах контрольных мероприятий, проведенных на значимом объекте критической информационной инфраструктуры с использованием сертифицированных по требованиям безопасности информации программных и программно-аппаратных средств контроля)

В ходе проведения проверки:

выявлены нарушения требований по обеспечению безопасности):

_____;

(описание выявленных нарушений)

выявлены факты невыполнения предписания органа государственного контроля об устранении выявленного нарушения требований по обеспечению безопасности (с указанием реквизитов выданного предписания): _____;

выявлены нарушения требований по обеспечению безопасности или факты, явившиеся причиной возникновения компьютерного инцидента, повлекшего негативные последствия, на значимом объекте критической информационной инфраструктуры:

_____;

нарушений требований по обеспечению безопасности не выявлено.

Рекомендации: _____.

Запись в Журнал учета проверок внесена:

_____	_____
(подпись должностного лица, проводившего проверку)	(подпись руководителя субъекта критической информационной инфраструктуры или уполномоченного им должностного лица)

Журнал учета проверок отсутствует:

_____	_____
(подпись должностного лица, проводившего проверку)	(подпись руководителя субъекта критической информационной инфраструктуры или уполномоченного им должностного лица)

Прилагаемые к акту документы: _____.

Подпись (подписи) должностного лица (должностных лиц) органа государственного контроля, проводившего (проводивших) проверку:

_____

С актом проверки ознакомлен(а), акт проверки со всеми приложениями получил(а):

_____

(фамилия, имя, отчество (последнее - при наличии) и должность руководителя субъекта критической информационной инфраструктуры или уполномоченного им должностного лица)

"__" _____ 20__ г. _____

(подпись)

Пометка об отказе ознакомления с актом проверки: _____

(подпись должностного лица органа государственного контроля, проводившего проверку)

Зарегистрировано в Минюсте России 22 февраля 2018 г. N 50118

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ПРИКАЗ
от 21 декабря 2017 г. N 235

ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ К СОЗДАНИЮ СИСТЕМ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ И ОБЕСПЕЧЕНИЮ ИХ ФУНКЦИОНИРОВАНИЯ

В соответствии с пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" (Собрание законодательства Российской Федерации, 2017, N 31, ст. 4736) приказываю:

Утвердить прилагаемые Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования.

Директор Федеральной службы
по техническому и экспортному контролю В.СЕЛИН

Утверждены
приказом ФСТЭК России
от 21 декабря 2017 г. N 235

ТРЕБОВАНИЯ
К СОЗДАНИЮ СИСТЕМ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ И ОБЕСПЕЧЕНИЮ ИХ ФУНКЦИОНИРОВАНИЯ

I. Общие положения

1. Настоящие Требования разработаны в соответствии с Федеральным законом от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" и устанавливают требования к созданию субъектами критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура) систем безопасности значимых объектов критической информационной инфраструктуры (далее - системы безопасности) и по обеспечению их функционирования.

2. Системы безопасности создаются субъектами критической информационной инфраструктуры и включают в себя правовые, организационные, технические и иные меры, направленные на обеспечение информационной безопасности (защиты информации) субъектов критической информационной инфраструктуры.

3. Создание и функционирование систем безопасности должно быть направлено на обеспечение устойчивого функционирования значимых объектов критической информационной инфраструктуры при проведении в отношении них компьютерных атак.

Системы безопасности создаются в отношении всех значимых объектов критической информационной инфраструктуры субъектов критической информационной инфраструктуры. По решению субъекта критической информационной инфраструктуры для одного или группы значимых объектов критической информационной инфраструктуры могут создаваться отдельные системы безопасности.

4. Системы безопасности включают силы обеспечения безопасности значимых объектов критической информационной инфраструктуры и используемые ими средства обеспечения безопасности значимых объектов критической информационной инфраструктуры.

К силам обеспечения безопасности значимых объектов критической информационной инфраструктуры относятся:

подразделения (работники) субъекта критической информационной инфраструктуры, ответственные за обеспечение безопасности значимых объектов критической информационной инфраструктуры;

подразделения (работники), эксплуатирующие значимые объекты критической информационной инфраструктуры;

подразделения (работники), обеспечивающие функционирование (сопровождение, обслуживание, ремонт) значимых объектов критической информационной инфраструктуры;

иные подразделения (работники), участвующие в обеспечении безопасности значимых объектов критической информационной инфраструктуры.

К средствам обеспечения безопасности значимых объектов критической информационной инфраструктуры относятся программные и программно-аппаратные средства, применяемые для обеспечения безопасности значимых объектов критической информационной инфраструктуры.

5. Системы безопасности должны функционировать в соответствии с организационно-распорядительными документами по обеспечению безопасности значимых объектов критической информационной инфраструктуры, разрабатываемыми субъектами критической информационной инфраструктуры в соответствии с настоящими Требованиями (далее - организационно-распорядительные документы по безопасности значимых объектов).

6. Системы безопасности должны обеспечивать:

предотвращение неправомерного доступа к информации, обрабатываемой значимыми объектами критической информационной инфраструктуры, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;

недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимых объектов критической информационной инфраструктуры;

восстановление функционирования значимых объектов критической информационной инфраструктуры, в том числе за счет создания и хранения резервных копий необходимой для этого информации;

непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, которое осуществляется в соответствии со статьей 5 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации".

7. Создаваемые системы безопасности должны соответствовать требованиям, предъявляемым к:

силам обеспечения безопасности значимых объектов критической информационной инфраструктуры;

программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов критической информационной инфраструктуры;

организационно-распорядительным документам по безопасности значимых объектов;

функционированию системы безопасности в части организации работ по обеспечению безопасности значимых объектов критической информационной инфраструктуры.

II. Требования к силам обеспечения безопасности значимых объектов критической информационной инфраструктуры

8. Руководитель субъекта критической информационной инфраструктуры или уполномоченное им лицо, на которое возложены функции обеспечения безопасности значимых объектов критической информационной инфраструктуры (далее - уполномоченное лицо), создает систему безопасности, организует и контролирует ее функционирование.

9. Руководитель субъекта критической информационной инфраструктуры определяет состав и структуру системы безопасности, а также функции ее участников при обеспечении безопасности значимых объектов критической информационной инфраструктуры в зависимости от количества значимых объектов критической информационной инфраструктуры, а также особенностей деятельности субъекта критической информационной инфраструктуры.

10. Руководитель субъекта критической информационной инфраструктуры создает или определяет структурное подразделение, ответственное за обеспечение безопасности значимых объектов критической информационной инфраструктуры (далее - структурное подразделение по безопасности), или назначает отдельных работников, ответственных за обеспечение безопасности значимых объектов критической информационной инфраструктуры (далее - специалисты по безопасности).

Структурное подразделение по безопасности, специалисты по безопасности должны осуществлять следующие функции:

разрабатывать предложения по совершенствованию организационно-распорядительных документов по безопасности значимых объектов и представлять их руководителю субъекта критической информационной инфраструктуры (уполномоченному лицу);

проводить анализ угроз безопасности информации в отношении значимых объектов критической информационной инфраструктуры и выявлять уязвимости в них;

обеспечивать реализацию требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленных в соответствии со статьей 11

Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" (далее - требования по безопасности);

обеспечивать в соответствии с требованиями по безопасности реализацию организационных мер и применение средств защиты информации, эксплуатацию средств защиты информации;

осуществлять реагирование на компьютерные инциденты в порядке, установленном в соответствии с пунктом 6 части 4 статьи 6 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации";

организовывать проведение оценки соответствия значимых объектов критической информационной инфраструктуры требованиям по безопасности;

готовить предложения по совершенствованию функционирования систем безопасности, а также по повышению уровня безопасности значимых объектов критической информационной инфраструктуры.

Структурное подразделение по безопасности, специалисты по безопасности реализуют указанные функции во взаимодействии с подразделениями (работниками), эксплуатирующими значимые объекты критической информационной инфраструктуры, и подразделениями (работниками), обеспечивающими функционирование значимых объектов критической информационной инфраструктуры.

11. Для выполнения функций, предусмотренных пунктом 10 настоящих Требований, субъектами критической информационной инфраструктуры могут привлекаться организации, имеющие в зависимости от информации, обрабатываемой значимым объектом критической информационной инфраструктуры, лицензию на деятельность по технической защите информации, составляющей государственную тайну, и (или) на деятельность по технической защите конфиденциальной информации (далее - лицензии в области защиты информации).

12. Работники структурного подразделения по безопасности, специалисты по безопасности должны обладать знаниями и навыками, необходимыми для обеспечения безопасности значимых объектов критической информационной инфраструктуры в соответствии с настоящими Требованиями и требованиями по безопасности.

13. Не допускается возложение на структурное подразделение по безопасности, специалистов по безопасности функций, не связанных с обеспечением безопасности значимых объектов критической информационной инфраструктуры или обеспечением информационной безопасности субъекта критической информационной инфраструктуры в целом.

Обязанности, возлагаемые на работников структурного подразделения по безопасности, специалистов по безопасности, должны быть определены в их должностных регламентах (инструкциях).

14. Подразделения, эксплуатирующие значимые объекты критической информационной инфраструктуры, должны обеспечивать безопасность эксплуатируемых ими значимых объектов критической информационной инфраструктуры. Объем возлагаемых на подразделения задач определяется субъектом критической информационной инфраструктуры в организационно-распорядительных документах по безопасности значимых объектов.

По решению субъекта критической информационной инфраструктуры в подразделениях, эксплуатирующих значимые объекты критической информационной инфраструктуры, могут также назначаться работники, на которых возлагаются отдельные функции по обеспечению безопасности значимых объектов критической информационной инфраструктуры. Обязанности, возлагаемые на работников, должны быть определены в их должностных регламентах (инструкциях).

Координацию и контроль деятельности указанных работников по вопросам обеспечения безопасности значимых объектов критической информационной инфраструктуры должны осуществлять структурное подразделение по безопасности, специалисты по безопасности.

15. Работники, эксплуатирующие значимые объекты критической информационной инфраструктуры (пользователи), а также работники, обеспечивающие функционирование значимых объектов критической информационной инфраструктуры, должны выполнять свои

обязанности на значимых объектах критической информационной инфраструктуры в соответствии с правилами безопасности, установленными организационно-распорядительными документами по безопасности значимых объектов (инструкциями, руководствами).

До работников должны быть доведены положения организационно-распорядительных документов по безопасности значимых объектов в части, их касающейся.

Субъект критической информационной инфраструктуры должен проводить не реже одного раза в год организационные мероприятия, направленные на повышение уровня знаний работников по вопросам обеспечения безопасности критической информационной инфраструктуры и о возможных угрозах безопасности информации.

16. Представители организаций, привлекаемых субъектом критической информационной инфраструктуры для эксплуатации, обеспечения функционирования значимых объектов критической информационной инфраструктуры и (или) для обеспечения их безопасности, должны быть ознакомлены с организационно-распорядительными документами по безопасности значимых объектов.

III. Требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов критической информационной инфраструктуры

17. К программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов критической информационной инфраструктуры, относятся средства защиты информации, в том числе средства защиты информации от несанкционированного доступа (включая встроенные в общесистемное, прикладное программное обеспечение), межсетевые экраны, средства обнаружения (предотвращения) вторжений (компьютерных атак), средства антивирусной защиты, средства (системы) контроля (анализа) защищенности, средства управления событиями безопасности, средства защиты каналов передачи данных.

18. Для обеспечения безопасности значимых объектов критической информационной инфраструктуры должны применяться сертифицированные на соответствие требованиям по безопасности средства защиты информации или средства, прошедшие оценку соответствия в форме испытаний или приемки в соответствии с Федеральным законом от 27 декабря 2002 г. N 184-ФЗ "О техническом регулировании" (Собрание законодательства Российской Федерации, 2002, N 52, ст. 5140; 2005, N 19, ст. 1752; 2007, N 19, ст. 2293; N 49, ст. 6070; 2008, N 30, ст. 3616; 2009, N 29, ст. 3626; N 48, ст. 5711; 2010, N 1, ст. 5, 6; N 40, ст. 4969; 2011, N 30, ст. 4603; N 49, ст. 7025; N 50, ст. 7351; 2012, N 31, ст. 4322; N 50, ст. 6959; 2013, N 27, ст. 3477; N 30, ст. 4071; N 52, ст. 6961; 2014, N 26, ст. 3366; 2015, N 17, ст. 2477; N 27, ст. 3951; N 29, ст. 4342; N 48, ст. 6724; 2016, N 15, ст. 2066).

Сертифицированные средства защиты информации применяются в случаях, установленных законодательством Российской Федерации, а также в случае принятия решения субъектом критической информационной инфраструктуры.

В иных случаях применяются средства защиты информации, прошедшие оценку соответствия в форме испытаний или приемки, которые проводятся субъектами критической информационной инфраструктуры самостоятельно или с привлечением организаций, имеющих в соответствии с законодательством Российской Федерации лицензии на деятельность в области защиты информации.

19. Параметры и характеристики применяемых средств защиты информации должны обеспечивать реализацию технических мер по обеспечению безопасности значимых объектов критической информационной инфраструктуры, принимаемыми в соответствии с требованиями по безопасности.

В качестве средств защиты информации в приоритетном порядке подлежат применению средства защиты информации, встроенные в программное обеспечение и (или) программно-

аппаратные средства значимых объектов критической информационной инфраструктуры (при их наличии).

20. Средства защиты информации должны применяться в соответствии с инструкциями (правилами) по эксплуатации, разработанными разработчиками (производителями) этих средств, и иной эксплуатационной документацией на средства защиты информации.

21. Применяемые средства защиты информации должны быть обеспечены гарантийной, технической поддержкой со стороны разработчиков (производителей).

При выборе средств защиты информации должно учитываться возможное наличие ограничений со стороны разработчиков (производителей) или иных лиц на применение этих средств на любом из принадлежащих субъекту критической информационной инфраструктуры значимых объектов критической информационной инфраструктуры.

22. Порядок применения средств защиты информации определяется субъектом критической информационной инфраструктуры в организационно-распорядительных документах по безопасности значимых объектов с учетом особенностей деятельности субъекта критической информационной инфраструктуры.

IV. Требования к организационно-распорядительным документам по безопасности значимых объектов

23. Субъектом критической информационной инфраструктуры в рамках функционирования системы безопасности должны быть утверждены организационно-распорядительные документы по безопасности значимых объектов, определяющие порядок и правила функционирования системы безопасности значимых объектов, а также порядок и правила обеспечения безопасности значимых объектов критической информационной инфраструктуры.

Организационно-распорядительные документы по безопасности значимых объектов являются частью документов по вопросам обеспечения информационной безопасности (защиты информации) субъекта критической информационной инфраструктуры. При этом положения, определяющие порядок и правила обеспечения безопасности значимых объектов критической информационной инфраструктуры, могут быть включены в общие документы по вопросам обеспечения информационной безопасности (защиты информации), а также могут являться частью документов по вопросам функционирования значимого объекта критической информационной инфраструктуры.

24. Организационно-распорядительные документы по безопасности значимых объектов разрабатываются исходя из особенностей деятельности субъекта критической информационной инфраструктуры на основе настоящих Требований, требований по безопасности, иных нормативных правовых актов в области обеспечения безопасности критической информационной инфраструктуры и защиты информации.

25. Организационно-распорядительные документы по безопасности значимых объектов должны определять:

а) цели и задачи обеспечения безопасности значимых объектов критической информационной инфраструктуры, основные угрозы безопасности информации и категории нарушителей, основные организационные и технические мероприятия по обеспечению безопасности значимых объектов критической информационной инфраструктуры, проводимые субъектом критической информационной инфраструктуры, состав и структуру системы безопасности и функции ее участников, порядок применения, формы оценки соответствия значимых объектов критической информационной инфраструктуры и средств защиты информации требованиям по безопасности;

б) планы мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры, модели угроз безопасности информации в отношении значимых объектов критической информационной инфраструктуры, порядок реализации отдельных мер по обеспечению безопасности значимых объектов критической

информационной инфраструктуры, порядок проведения испытаний или приемки средств защиты информации, порядок реагирования на компьютерные инциденты, порядок информирования и обучения работников, порядок взаимодействия подразделений (работников) субъекта критической информационной инфраструктуры при решении задач обеспечения безопасности значимых объектов критической информационной инфраструктуры, порядок взаимодействия субъекта критической информационной инфраструктуры с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

в) правила безопасной работы работников субъекта критической информационной инфраструктуры на значимых объектах критической информационной инфраструктуры, действия работников субъекта критической информационной инфраструктуры при возникновении компьютерных инцидентов и иных нештатных ситуаций.

Состав и формы организационно-распорядительных документов по безопасности значимых объектов определяются субъектом критической информационной инфраструктуры с учетом особенностей его деятельности.

26. Организационно-распорядительные документы по безопасности значимых объектов утверждаются руководителем субъекта критической информационной инфраструктуры (уполномоченным лицом). По решению руководителя субъекта критической информационной инфраструктуры отдельные организационно-распорядительные документы по безопасности значимых объектов могут утверждаться иными уполномоченными на это лицами субъекта критической информационной инфраструктуры.

27. Организационно-распорядительные документы по безопасности значимых объектов должны быть доведены до руководства субъекта критической информационной инфраструктуры, подразделения по безопасности, специалистов по безопасности, а также до иных подразделений (работников), участвующих в обеспечении безопасности значимых объектов критической информационной инфраструктуры, в части, их касающейся.

V. Требования к функционированию системы безопасности в части организации работ по обеспечению безопасности значимых объектов критической информационной инфраструктуры

28. В рамках функционирования системы безопасности субъектом критической информационной инфраструктуры должны быть внедрены следующие процессы:

планирование и разработка мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры;

реализация (внедрение) мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры;

контроль состояния безопасности значимых объектов критической информационной инфраструктуры;

совершенствование безопасности значимых объектов критической информационной инфраструктуры.

29. В рамках планирования мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры осуществляются разработка и утверждение ежегодного плана мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры (далее - план мероприятий).

По решению субъекта критической информационной инфраструктуры план мероприятий может разрабатываться на более длительный срок с учетом имеющихся программ (планов) по модернизации, оснащению значимых объектов критической информационной инфраструктуры.

План мероприятий разрабатывается структурным подразделением по безопасности, специалистами по безопасности с участием подразделений (работников), эксплуатирующих значимые объекты критической информационной инфраструктуры, и подразделений

(работников), обеспечивающих функционирование значимых объектов критической информационной инфраструктуры.

30. План мероприятий должен содержать наименования мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры, сроки их выполнения, наименования подразделений (работников), ответственных за реализацию каждого мероприятия.

В план мероприятий включаются мероприятия по обеспечению функционирования системы безопасности, а также организационные и технические мероприятия по обеспечению безопасности значимых объектов критической информационной инфраструктуры, направленные на решение задач, установленных пунктом 6 настоящих Требований.

31. Разработка мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры осуществляется в соответствии с настоящими Требованиями, требованиями по безопасности, иными нормативными правовыми актами по обеспечению безопасности критической информационной инфраструктуры, а также организационно-распорядительными документами по безопасности значимых объектов.

План мероприятий утверждается руководителем субъекта критической информационной инфраструктуры и доводится до подразделений (работников) субъекта критической информационной инфраструктуры в части, их касающейся.

В подразделениях, эксплуатирующих значимые объекты критической информационной инфраструктуры, и подразделениях, обеспечивающих функционирование значимых объектов критической информационной инфраструктуры, на основе утвержденного плана мероприятий могут разрабатываться соответствующие отдельные планы мероприятий.

32. Контроль за выполнением плана мероприятий осуществляется структурным подразделением по безопасности, специалистами по безопасности. Структурное подразделение по безопасности, специалисты по безопасности ежегодно должны готовить отчет о выполнении плана мероприятий, который представляется руководителю субъекта критической информационной инфраструктуры.

33. Мероприятия по обеспечению безопасности значимых объектов критической информационной инфраструктуры могут включаться в общий план деятельности субъекта критической информационной инфраструктуры (в случае его разработки) отдельным разделом.

Порядок разработки, утверждения и внесения изменений в план мероприятий определяется субъектом критической информационной инфраструктуры в организационно-распорядительных документах по безопасности значимых объектов.

34. Реализация (внедрение) мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры является результатом выполнения плана мероприятий и осуществляется в соответствии с организационно-распорядительными документами по безопасности значимых объектов.

В ходе реализации мероприятий по обеспечению безопасности значимых объектов должны приниматься организационные меры и (или) внедряться средства защиты информации на значимых объектах критической информации, направленные на блокирование (нейтрализацию) угроз безопасности информации.

Результаты реализации мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры подлежат документированию в порядке, установленном субъектом критической информационной инфраструктуры в организационно-распорядительных документах по безопасности значимых объектов.

35. В рамках контроля состояния безопасности значимых объектов критической информационной инфраструктуры должен осуществляться внутренний контроль организации работ по обеспечению безопасности значимых объектов критической информационной инфраструктуры и эффективности принимаемых организационных и технических мер.

В ходе проведения контроля проверяется выполнение настоящих Требований, требований по безопасности, иных нормативных правовых актов в области обеспечения безопасности

критической информационной инфраструктуры, а также организационно-распорядительных документов по безопасности значимых объектов.

36. Контроль проводится ежегодно комиссией, назначаемой субъектом критической информационной инфраструктуры. В состав комиссии включаются работники структурного подразделения по безопасности, специалисты по безопасности, работники подразделений, эксплуатирующих значимые объекты критической информационной инфраструктуры, и подразделений, обеспечивающих функционирование значимых объектов критической информационной инфраструктуры. По решению субъекта критической информационной инфраструктуры в состав комиссии могут включаться работники иных подразделений субъекта критической информационной инфраструктуры.

Для оценки эффективности принятых организационных и технических мер по обеспечению безопасности значимых объектов критической информационной инфраструктуры могут применяться средства контроля (анализа) защищенности.

Результаты контроля оформляются актом, который подписывается членами комиссии и утверждается руководителем субъекта критической информационной инфраструктуры (уполномоченным лицом).

В случае проведения по решению руководителя субъекта критической информационной инфраструктуры внешней оценки (внешнего аудита) состояния безопасности значимых объектов критической информационной инфраструктуры внутренний контроль может не проводиться.

Для проведения внешней оценки привлекаются организации, имеющие лицензии на деятельность в области защиты информации (в части услуг по контролю защищенности информации от несанкционированного доступа и ее модификации в средствах и системах информатизации).

Замечания, выявленные по результатам внутреннего контроля или внешней оценки (внешнего аудита), подлежат устранению в порядке и сроки, установленные руководителем субъекта критической информационной инфраструктуры (уполномоченным лицом).

37. В рамках совершенствования безопасности значимых объектов критической информационной инфраструктуры структурное подразделение по безопасности, специалисты по безопасности должны проводить анализ функционирования системы безопасности и состояния безопасности значимых объектов критической информационной инфраструктуры, по результатам которого разрабатывать предложения по развитию системы безопасности и меры по совершенствованию безопасности значимых объектов критической информационной инфраструктуры.

Анализ функционирования системы безопасности, а также разработка предложений по совершенствованию безопасности значимых объектов критической информационной инфраструктуры осуществляются структурным подразделением по безопасности, специалистами по безопасности с участием подразделений (работников), эксплуатирующих значимые объекты критической информационной инфраструктуры, и подразделений (работников), обеспечивающих функционирование значимых объектов критической информационной инфраструктуры.

Предложения по совершенствованию безопасности значимых объектов критической информационной инфраструктуры представляются руководителю субъекта критической информационной инфраструктуры (уполномоченному лицу).

В соответствии с решением руководителя субъекта критической информационной инфраструктуры (уполномоченного лица) предложения по совершенствованию безопасности значимых объектов критической информационной инфраструктуры включаются в план мероприятий, разрабатываемый в соответствии с пунктами 29 - 33 настоящих Требований.

Зарегистрировано в Минюсте России

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ПРИКАЗ
от 21 декабря 2017 г. N 236
ОБ УТВЕРЖДЕНИИ ФОРМЫ НАПРАВЛЕНИЯ СВЕДЕНИЙ О РЕЗУЛЬТАТАХ ПРИСВОЕНИЯ ОБЪЕКТУ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ОДНОЙ ИЗ КАТЕГОРИЙ ЗНАЧИМОСТИ ЛИБО ОБ ОТСУТСТВИИ НЕОБХОДИМОСТИ ПРИСВОЕНИЯ ЕМУ ОДНОЙ ИЗ ТАКИХ КАТЕГОРИЙ

В соответствии с пунктом 3 части 3 статьи 6 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" (Собрание законодательства Российской Федерации, 2017, N 31, ст. 4736) приказываю:

Утвердить прилагаемую форму направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий.

Директор Федеральной службы
по техническому и экспортному контролю В.СЕЛИН

Утверждена
приказом ФСТЭК России
от 22 декабря 2017 г. N 236

Форма

Сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий

Ограничительная пометка
или гриф секретности
(при необходимости)

В Федеральную службу по техническому и экспортному контролю

1. Сведения об объекте критической информационной инфраструктуры

1.1.	Наименование объекта	
1.2.	Адреса размещения объекта, в том числе адреса обособленных подразделений, филиалов, представительств субъекта критической информационной инфраструктуры, в которых размещаются сегменты распределенного объекта (серверы, рабочие места, технологическое, производственное оборудование (исполнительные устройства)	
1.3.	Сфера (область) деятельности, в которой функционирует объект, в соответствии с пунктом 8 статьи 2 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"	
1.4.	Назначение объекта	
1.5.	Критические процессы (управленческие, технологические, производственные, финансово-экономические и (или) иные процессы, функции управления и контроля), которые обеспечиваются объектом	
1.6.	Архитектура объекта (одноранговая сеть, клиент-серверная система, технология "тонкий клиент", сеть передачи данных, система диспетчерского управления и контроля, распределенная система управления, иная архитектура)	

2. Сведения о субъекте критической информационной инфраструктуры

2.1.	Наименование субъекта	
2.2.	Адрес местонахождения субъекта	
2.3.	Должность, фамилия, имя, отчество (при наличии) руководителя субъекта	

2.4.	Должность, фамилия, имя, отчество (при наличии) должностного лица, на которое возложены функции обеспечения безопасности значимых объектов, или в случае отсутствия такого должностного лица, наименование должности, фамилия, имя, отчество (при наличии) руководителя субъекта.	
2.5.	Структурное подразделение, ответственное за обеспечение безопасности значимых объектов, должность, фамилия, имя, отчество (при наличии) руководителя структурного подразделения, телефон, адрес электронной почты (при наличии) или должность, фамилия, имя, отчество (при наличии) штатного специалиста, ответственного за обеспечение безопасности значимых объектов, телефон, адрес электронной почты (при наличии)	

3. Сведения о взаимодействии объекта критической информационной инфраструктуры и сетей электросвязи

3.1.	Категория сети электросвязи (общего пользования, выделенная, технологическая, присоединенная к сети связи общего пользования, специального назначения, другая сеть связи для передачи информации при помощи электромагнитных систем) или сведения об отсутствии взаимодействия объекта критической информационной инфраструктуры с сетями электросвязи	
3.2.	Наименование оператора связи	
3.3.	Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель)	
3.4.	Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), используемых технологий доступа, протоколов взаимодействия	

4. Сведения о лице, эксплуатирующем объект критической информационной инфраструктуры

4.1.	Наименование юридического лица или фамилия, имя, отчество (при наличии) индивидуального предпринимателя, эксплуатирующего объект	
4.2.	Адрес местонахождения юридического лица или адрес места жительства индивидуального предпринимателя, эксплуатирующего объект	
4.3.	Элемент (компонент) объекта, который эксплуатируется лицом (центр обработки данных, серверное оборудование, телекоммуникационное оборудование, технологическое, производственное оборудование (исполнительные	

	устройства), иные элементы (компоненты)	

5. Сведения о программных и программно-аппаратных средствах, используемых на объекте критической информационной инфраструктуры

5.1.	Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, технологического, производственного оборудования (исполнительных устройств), иных средств) и их количество	
5.2.	Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии)	
5.3.	Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем)	
5.4.	Применяемые средства защиты информации (наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о непроведении такой оценки; функции безопасности программного обеспечения, если в него встроены средства защиты информации (идентификация, аутентификация, управление доступом, регистрация событий безопасности, фильтрация, иные функции) или сведения об отсутствии средств защиты информации.	

6. Сведения об угрозах безопасности информации и категориях нарушителей в отношении объекта критической информационной инфраструктуры

6.1.	Категория нарушителя (внешний или внутренний), краткая характеристика основных возможностей нарушителя по реализации угроз безопасности информации в части его оснащенности, знаний, мотивации или краткое обоснование невозможности нарушителем реализовать угрозы безопасности информации	
6.2.	Основные угрозы безопасности информации или обоснование их неактуальности	

7. Возможные последствия в случае возникновения компьютерных инцидентов

7.1.	Типы компьютерных инцидентов, которые могут произойти в результате реализации угроз безопасности информации, в том числе вследствие целенаправленных компьютерных атак (отказ в обслуживании, несанкционированный доступ, утечка данных (нарушение	

	конфиденциальности), модификация (подмена) данных, нарушение функционирования технических средств, несанкционированное использование вычислительных ресурсов объекта), или обоснование невозможности наступления компьютерных инцидентов	
7.2.	Ущерб, который может быть причинен в результате возникновения компьютерных инцидентов, в соответствии с показателями критериев значимости, утверждаемыми в соответствии с пунктом 1 части 2 статьи 6 Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" или обоснование отсутствия возможности причинения ущерба вследствие компьютерных инцидентов	

8. Категория значимости, которая присвоена объекту критической информационной инфраструктуры

8.1.	Категория значимости, которая присвоена объекту	
8.2.	Полученные значения по каждому из показателей критериев значимости с обоснованием или информация о неприменимости показателя к объекту с соответствующим обоснованием	

9. Организационные и технические меры, применяемые для обеспечения безопасности значимого объекта критической информационной инфраструктуры

9.1.	Организационные меры (установление контролируемой зоны, контроль физического доступа к объекту, разработка документов (регламентов, инструкций, руководств) по обеспечению безопасности объекта)	
9.2.	Технические меры по идентификации и аутентификации, управлению доступом, ограничению программной среды, антивирусной защите и иные в соответствии с требованиями по обеспечению безопасности значимых объектов	

_____ _____ _____

(Наименование должности руководителя субъекта критической информационной инфраструктуры или уполномоченного им лица) (подпись) (инициалы, фамилия)

М.П. (при наличии печати)

"__" _____ 20__ г

.

Зарегистрировано в Минюсте России 26 марта 2018 г. N 50524

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ПРИКАЗ
от 21 декабря 2017 г. N 239

ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

(в ред. Приказа ФСТЭК России от 09.08.2018 N 138)

В соответствии с пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" (Собрание законодательства Российской Федерации, 2017, N 31, ст. 4736) приказываю:

Утвердить прилагаемые Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации.

Директор Федеральной службы
по техническому и экспортному контролю В.СЕЛИН

Утверждены
приказом ФСТЭК России
от 25 декабря 2017 г. N 239

ТРЕБОВАНИЯ
ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

(в ред. Приказа ФСТЭК России от 09.08.2018 N 138)

I. Общие положения

1. Настоящие Требования разработаны в соответствии с Федеральным законом от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" и направлены на обеспечение устойчивого функционирования значимых объектов критической информационной инфраструктуры Российской Федерации (далее - значимые объекты, критическая информационная инфраструктура) при проведении в отношении них компьютерных атак.

2. Действие настоящих Требований распространяется на информационные системы, автоматизированные системы управления, информационно-телекоммуникационные сети, которые отнесены к значимым объектам критической информационной инфраструктуры в соответствии со статьей 7 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".

3. По решению субъекта критической информационной инфраструктуры настоящие Требования могут применяться для обеспечения безопасности объектов критической информационной инфраструктуры, не отнесенных к значимым объектам.

4. Обеспечение безопасности значимых объектов, в которых обрабатывается информация, составляющая государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

5. Для обеспечения безопасности значимых объектов, являющихся информационными системами персональных данных, настоящие Требования применяются с учетом Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 (Собрание законодательства Российской Федерации, 2012, N 45, ст. 6257).

Для обеспечения безопасности значимых объектов, являющихся государственными информационными системами, настоящие Требования применяются с учетом Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. N 17 (зарегистрирован Минюстом России 31 мая 2013 г., регистрационный N 28608) (с изменениями, внесенными приказом ФСТЭК России от 15 февраля 2017 г. N 27 "О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11 февраля 2013 г. N 17" (зарегистрирован Минюстом России 14 марта 2017 г., регистрационный N 45933).

6. Безопасность значимых объектов обеспечивается субъектами критической информационной инфраструктуры в рамках функционирования систем безопасности значимых объектов, создаваемых субъектами критической информационной инфраструктуры в соответствии со статьей 10 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".

II. Требования к обеспечению безопасности в ходе создания, эксплуатации и вывода из эксплуатации значимых объектов

7. Обеспечение безопасности значимых объектов является составной частью работ по созданию (модернизации), эксплуатации и вывода из эксплуатации значимых объектов. Меры по обеспечению безопасности значимых объектов принимаются на всех стадиях (этапах) их жизненного цикла.

8. На стадиях (этапах) жизненного цикла в ходе создания (модернизации), эксплуатации и вывода из эксплуатации значимого объекта проводятся:

а) установление требований к обеспечению безопасности значимого объекта;

б) разработка организационных и технических мер по обеспечению безопасности значимого объекта;

в) внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие;

г) обеспечение безопасности значимого объекта в ходе его эксплуатации;

д) обеспечение безопасности значимого объекта при выводе его из эксплуатации.

Результаты реализации мероприятий, проводимых для обеспечения безопасности значимого объекта на стадиях (этапах) его жизненного цикла, подлежат документированию. Состав и формы документов определяются субъектом критической информационной инфраструктуры.

9. Для значимых объектов, находящихся в эксплуатации, настоящие Требования подлежат реализации в рамках модернизации или дооснащения подсистем безопасности эксплуатируемых значимых объектов. Модернизация или дооснащение подсистем безопасности значимых объектов осуществляется в порядке, установленном настоящими Требованиями для создания значимых объектов и их подсистем безопасности, с учетом имеющихся у субъектов критической информационной инфраструктуры программ (планов) по модернизации или дооснащению значимых объектов.

Установление требований к обеспечению безопасности значимого объекта

10. Задание требований к обеспечению безопасности значимого объекта осуществляется субъектом критической информационной инфраструктуры и (или) лицом, устанавливающим требования к обеспечению безопасности значимых объектов, в соответствии с категорией значимости значимого объекта, определенной в порядке, установленном Правилами категорирования объектов критической информационной инфраструктуры Российской Федерации, утвержденными постановлением Правительства Российской Федерации от 8 февраля 2018 г. N 127 "Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации" (Собрание законодательства Российской Федерации, 2018, N 8, ст. 1204).

Требования к обеспечению безопасности включаются в техническое задание на создание значимого объекта и (или) техническое задание (частное техническое задание) на создание подсистемы безопасности значимого объекта, которые должны содержать:

а) цель и задачи обеспечения безопасности значимого объекта или подсистемы безопасности значимого объекта;

б) категорию значимости значимого объекта;

в) перечень нормативных правовых актов, методических документов и национальных стандартов, которым должен соответствовать значимый объект;

г) перечень типов объектов защиты значимого объекта;

д) организационные и технические меры, применяемые для обеспечения безопасности значимого объекта;

е) стадии (этапы работ) создания подсистемы безопасности значимого объекта;

ж) требования к применяемым программным и программно-аппаратным средствам, в том числе средствам защиты информации;

з) требования к защите средств и систем, обеспечивающих функционирование значимого объекта (обеспечивающей инфраструктуре);

и) требования к информационному взаимодействию значимого объекта с иными объектами критической информационной инфраструктуры, а также иными информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями.

В случае если значимый объект создается в рамках объекта капитального строительства, требования к обеспечению безопасности значимого объекта задаются застройщиком и оформляются в виде приложения к заданию на проектирование (реконструкцию) объекта капитального строительства.

При определении требований к обеспечению безопасности значимого объекта учитываются положения организационно-распорядительных документов по обеспечению безопасности значимых объектов, разрабатываемых субъектами критической информационной инфраструктуры в соответствии с требованиями к созданию систем безопасности значимых объектов и обеспечению их функционирования, утвержденными в соответствии с пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" (далее - организационно-распорядительные документы по безопасности значимых объектов).

Разработка организационных и технических мер по обеспечению безопасности значимого объекта

11. Разработка организационных и технических мер по обеспечению безопасности значимого объекта осуществляется субъектом критической информационной инфраструктуры и (или) лицом, привлекаемым в соответствии с законодательством Российской Федерации к проведению работ по созданию (модернизации) значимого объекта и (или) обеспечению его безопасности, в соответствии с техническим заданием на создание значимого объекта и (или) техническим заданием (частным техническим заданием) на создание подсистемы безопасности значимого объекта и должна включать:

а) анализ угроз безопасности информации и разработку модели угроз безопасности информации или ее уточнение (при ее наличии);

б) проектирование подсистемы безопасности значимого объекта;

в) разработку рабочей (эксплуатационной) документации на значимый объект (в части обеспечения его безопасности).

Разрабатываемые организационные и технические меры по обеспечению безопасности значимого объекта не должны оказывать негативного влияния на создание и функционирование значимого объекта.

При разработке организационных и технических мер по обеспечению безопасности значимого объекта учитывается его информационное взаимодействие с иными объектами критической информационной инфраструктуры, информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями.

11.1. Целью анализа угроз безопасности информации является определение возможных способов реализации (возникновения) угроз безопасности информации и последствий их реализации (возникновения) с учетом состава пользователей и их полномочий, программных и программно-аппаратных средств, взаимосвязей компонентов значимого объекта, взаимодействия с иными объектами критической информационной инфраструктуры, информационными системами, автоматизированными системами управления, информационно-телекоммуникационными сетями (далее - архитектура значимого объекта), а также

особенностей функционирования значимого объекта.

Анализ угроз безопасности информации должен включать:

а) выявление источников угроз безопасности информации и оценку возможностей (потенциала) внешних и внутренних нарушителей;

б) анализ возможных уязвимостей значимого объекта и его программных, программно-аппаратных средств;

в) определение возможных способов (сценариев) реализации (возникновения) угроз безопасности информации;

г) оценку возможных последствий от реализации (возникновения) угроз безопасности информации.

В качестве исходных данных для анализа угроз безопасности информации используется банк данных угроз безопасности информации, ведение которого осуществляется ФСТЭК России в соответствии с подпунктом 21 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085 (Собрание законодательства Российской Федерации, 2004, N 34, ст. 3541; 2006, N 49, ст. 5192; 2008, N 43, ст. 4921; N 47, ст. 5431; 2012, N 7, ст. 818; 2013, N 26, ст. 3314; N 53, ст. 7137; 2014, N 36, ст. 4833; N 44, ст. 6041; 2015, N 4, ст. 641; 2016, N 1, ст. 211; 2017, N 48, ст. 7198) (далее - банк данных угроз безопасности информации ФСТЭК России), а также источники, содержащие иные сведения об уязвимостях и угрозах безопасности информации.

По результатам анализа угроз безопасности информации могут быть разработаны рекомендации по корректировке архитектуры значимого объекта и организационно-распорядительных документов по безопасности значимых объектов, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

Модель угроз безопасности информации должна содержать краткое описание архитектуры значимого объекта, характеристику источников угроз безопасности информации, в том числе модель нарушителя, и описание всех угроз безопасности информации, актуальных для значимого объекта.

Описание каждой угрозы безопасности информации должно включать:

а) источник угрозы безопасности информации;

б) уязвимости (ошибки), которые могут быть использованы для реализации (способствовать возникновению) угрозы безопасности информации;

в) возможные способы (сценарии) реализации угрозы безопасности информации;

г) возможные последствия от угрозы безопасности информации.

Модель угроз безопасности информации может разрабатываться для нескольких значимых объектов, имеющих одинаковые цели создания и архитектуру, а также типовые угрозы безопасности информации.

Для определения угроз безопасности информации и разработки модели угроз безопасности информации должны применяться методические документы, разработанные и утвержденные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085.

11.2. Проектирование подсистемы безопасности значимого объекта должно осуществляться в соответствии с техническим заданием на создание значимого объекта и (или) техническим заданием (частным техническим заданием) на создание подсистемы безопасности значимого объекта с учетом модели угроз безопасности информации и категории значимости значимого объекта.

При проектировании подсистемы безопасности значимого объекта:

а) определяются субъекты доступа (пользователи, процессы и иные субъекты доступа) и объекты доступа;

б) определяются политики управления доступом (дискреционная, мандатная, ролевая, комбинированная);

в) обосновываются организационные и технические меры, подлежащие реализации в рамках подсистемы безопасности значимого объекта;

г) определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер по обеспечению безопасности значимого объекта;

д) осуществляется выбор средств защиты информации и (или) их разработка с учетом категории значимости значимого объекта, совместимости с программными и программно-аппаратными средствами, выполняемых функций безопасности и ограничений на эксплуатацию;

е) разрабатывается архитектура подсистемы безопасности значимого объекта, включающая состав, места установки, взаимосвязи средств защиты информации;

ж) определяются требования к параметрам настройки программных и программно-аппаратных средств, включая средства защиты информации, обеспечивающие реализацию мер по обеспечению безопасности, блокирование (нейтрализацию) угроз безопасности информации и устранение уязвимостей значимого объекта;

з) определяются меры по обеспечению безопасности при взаимодействии значимого объекта с иными объектами критической информационной инфраструктуры, информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями.

В случае если в ходе проектирования подсистемы безопасности значимого объекта предусмотрена разработка программного обеспечения, в том числе программного обеспечения средств защиты информации, такая разработка проводится в соответствии со стандартами безопасной разработки программного обеспечения.

Результаты проектирования подсистемы безопасности значимого объекта отражаются в проектной документации на значимый объект (подсистему безопасности значимого объекта).

В целях тестирования подсистемы безопасности значимого объекта в ходе проектирования может осуществляться ее макетирование или создание тестовой среды. Тестирование должно быть направлено на:

обеспечение работоспособности и совместимости выбранных средств защиты информации с программными и аппаратными средствами значимого объекта;

практическую отработку выполнения средствами защиты информации функций безопасности;

исключение влияния подсистемы безопасности на функционирование значимого объекта.

Макетирование подсистемы безопасности значимого объекта и ее тестирование может проводиться с использованием средств и методов моделирования, а также с использованием технологий виртуализации.

При проектировании подсистем безопасности значимых объектов, являющихся информационно-телекоммуникационными сетями, настоящие Требования применяются с учетом Требований к проектированию сетей электросвязи, утвержденных приказом Минкомсвязи России от 9 марта 2017 г. N 101 (зарегистрирован Минюстом России 31 мая 2017 г., регистрационный N 46915), а также иных нормативных правовых актов федерального органа исполнительной власти, осуществляющего функции по выработке и реализации государственной политики и нормативно-правовому регулированию в области связи.

11.3. Разработка рабочей (эксплуатационной) документации на значимый объект осуществляется в соответствии с техническим заданием на создание значимого объекта и (или) техническим заданием (частным техническим заданием) на создание подсистемы безопасности значимого объекта на основе проектной документации.

Рабочая (эксплуатационная) документация на значимый объект должна содержать:

описание архитектуры подсистемы безопасности значимого объекта;

порядок и параметры настройки программных и программно-аппаратных средств, в том числе средств защиты информации;

правила эксплуатации программных и программно-аппаратных средств, в том числе средств защиты информации (правила безопасной эксплуатации).

Состав и формы рабочей (эксплуатационной) документации определяются в соответствии с техническим заданием на создание значимого объекта и (или) техническим заданием (частным техническим заданием) на создание подсистемы безопасности значимого объекта.

Внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие

12. Внедрение организационных и технических мер по обеспечению безопасности значимого объекта организуется субъектом критической информационной инфраструктуры в соответствии с проектной и рабочей (эксплуатационной) документацией на значимый объект, стандартами организаций и включает:

а) установку и настройку средств защиты информации, настройку программных и программно-аппаратных средств;

б) разработку организационно-распорядительных документов, регламентирующих правила и процедуры обеспечения безопасности значимого объекта;

в) внедрение организационных мер по обеспечению безопасности значимого объекта;

г) предварительные испытания значимого объекта и его подсистемы безопасности;

д) опытную эксплуатацию значимого объекта и его подсистемы безопасности;

е) анализ уязвимостей значимого объекта и принятие мер по их устранению;

ж) приемочные испытания значимого объекта и его подсистемы безопасности.

По решению субъекта критической информационной инфраструктуры к разработке и внедрению организационных и технических мер по обеспечению безопасности значимого объекта может привлекаться лицо, эксплуатирующее (планирующее эксплуатировать) значимый объект.

12.1. Установка и настройка средств защиты информации должна проводиться в соответствии с проектной и рабочей (эксплуатационной) документацией на значимый объект, а также в соответствии с эксплуатационной документацией на отдельные средства защиты информации.

При установке и настройке средств защиты информации должно быть обеспечено выполнение ограничений на эксплуатацию этих средств защиты информации, в случае их наличия в эксплуатационной документации.

12.2. Разрабатываемые организационно-распорядительные документы по безопасности значимого объекта должны определять правила и процедуры реализации отдельных организационных и (или) технических мер (политик безопасности), разработанных и внедренных в рамках подсистемы безопасности значимого объекта в соответствии с главой III настоящих Требований.

Организационно-распорядительные документы по безопасности значимого объекта должны в том числе устанавливать правила безопасной работы работников, эксплуатирующих значимые объекты, и работников, обеспечивающих функционирование значимых объектов, а также действия работников при возникновении нештатных ситуаций, в том числе вызванных компьютерными инцидентами.

Состав и формы организационно-распорядительных документов по безопасности значимых объектов определяются субъектом критической информационной инфраструктуры с учетом особенностей его деятельности.

12.3. При внедрении организационных мер по обеспечению безопасности значимого объекта осуществляются:

а) организация контроля физического доступа к программно-аппаратным средствам значимого объекта и его линиям связи;

б) реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации программных и программно-аппаратных средств;

в) проверка полноты и детальности описания в организационно-распорядительных документах по безопасности значимых объектов действий пользователей и администраторов значимого объекта по реализации организационных мер;

г) определение администратора безопасности значимого объекта;

д) отработка действий пользователей и администраторов значимого объекта по реализации мер по обеспечению безопасности значимого объекта.

12.4. Предварительные испытания значимого объекта и его подсистемы безопасности должны проводиться в соответствии с программой и методиками предварительных испытаний и включать проверку работоспособности подсистемы безопасности значимого объекта и отдельных средств защиты информации, оценку влияния подсистемы безопасности на функционирование значимого объекта при проектных режимах его работы, установленных проектной документацией, а также принятие решения о возможности опытной эксплуатации значимого объекта и его подсистемы безопасности.

12.5. Опытная эксплуатация значимого объекта и его подсистемы безопасности должна проводиться в соответствии с программой и методиками опытной эксплуатации и включать проверку функционирования подсистемы безопасности значимого объекта, в том числе реализованных организационных и технических мер, а также знаний и умений пользователей и администраторов, необходимых для эксплуатации значимого объекта и его подсистемы безопасности.

12.6. Анализ уязвимостей значимого объекта проводится в целях выявления недостатков (слабостей) в подсистеме безопасности значимого объекта и оценки возможности их использования для реализации угроз безопасности информации. При этом анализу подлежат уязвимости кода, конфигурации и архитектуры значимого объекта.

Анализ уязвимостей проводится для всех программных и программно-аппаратных средств, в том числе средств защиты информации, значимого объекта.

При проведении анализа уязвимостей применяются следующие способы их выявления:

а) анализ проектной, рабочей (эксплуатационной) документации и организационно-распорядительных документов по безопасности значимого объекта;

б) анализ настроек программных и программно-аппаратных средств, в том числе средств защиты информации, значимого объекта;

в) выявление известных уязвимостей программных и программно-аппаратных средств, в том числе средств защиты информации, посредством анализа состава установленного программного обеспечения и обновлений безопасности с применением средств контроля (анализа) защищенности и (или) иных средств защиты информации;

г) выявление известных уязвимостей программных и программно-аппаратных средств, в том числе средств защиты информации, сетевых служб, доступных для сетевого взаимодействия, с применением средств контроля (анализа) защищенности;

д) тестирование на проникновение в условиях, соответствующих возможностям нарушителей, определенных в модели угроз безопасности информации.

Применение способов и средств выявления уязвимостей осуществляется субъектом критической информационной инфраструктуры с учетом особенностей функционирования значимого объекта.

Допускается проведение анализа уязвимостей на макете (в тестовой зоне) значимого объекта или макетах отдельных сегментов значимого объекта.

Анализ уязвимостей значимого объекта проводится до ввода его в действие на этапах, определяемых субъектом критической информационной инфраструктуры.

В случае выявления уязвимостей значимого объекта, которые могут быть использованы для реализации (способствовать возникновению) угроз безопасности информации, принимаются меры, направленные на их устранение или исключающие возможность использования (эксплуатации) нарушителем выявленных уязвимостей.

По результатам анализа уязвимостей должно быть подтверждено, что в значимом объекте, отсутствуют уязвимости, как минимум содержащиеся в банке данных угроз безопасности

информации ФСТЭК России, указанном в пункте 11.1 настоящих Требований, или выявленные уязвимости не приводят к возникновению угроз безопасности информации в отношении значимого объекта.

12.7. В ходе приемочных испытаний значимого объекта и его подсистемы безопасности должен быть проведен комплекс организационных и технических мероприятий (испытаний), в результате которых подтверждается соответствие значимого объекта и его подсистемы безопасности настоящим Требованиям, а также требованиям технического задания на создание значимого объекта и (или) технического задания (частного технического задания) на создание подсистемы безопасности значимого объекта.

В качестве исходных данных при приемочных испытаниях используются модель угроз безопасности информации, результаты (акт) категорирования, техническое задание на создание (модернизацию) значимого объекта и (или) техническое задание (частное техническое задание) на создание подсистемы безопасности значимого объекта, проектная и рабочая (эксплуатационная) документация на значимый объект, организационно-распорядительные документы по безопасности значимых объектов, результаты анализа уязвимостей значимого объекта, материалы предварительных испытаний и опытной эксплуатации, а также иные документы, разрабатываемые в соответствии с настоящими Требованиями и требованиями стандартов организации.

Приемочные испытания значимого объекта и его подсистемы безопасности проводятся в соответствии с программой и методикой приемочных испытаний. Результаты приемочных испытаний значимого объекта и его подсистемы безопасности с выводом о ее соответствии установленным требованиям включаются в акт приемки значимого объекта в эксплуатацию.

В случае если значимый объект является государственной информационной системой, в иных случаях, установленных законодательством Российской Федерации, а также в случае принятия решения субъектом критической информационной инфраструктуры, оценка значимого объекта и его подсистемы безопасности проводится в форме аттестации значимого объекта в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 11 февраля 2013 г. N 17.

Ввод в действие значимого объекта и его подсистемы безопасности осуществляется при положительном заключении (выводе) в акте приемки (или в аттестате соответствия) о соответствии значимого объекта установленным требованиям по обеспечению безопасности.

Обеспечение безопасности значимого объекта в ходе его эксплуатации

13. Обеспечение безопасности в ходе эксплуатации значимого объекта осуществляется субъектом критической информационной инфраструктуры в соответствии с эксплуатационной документацией и организационно-распорядительными документами по безопасности значимого объекта и должно включать реализацию следующих мероприятий:

а) планирование мероприятий по обеспечению безопасности значимого объекта;

б) анализ угроз безопасности информации в значимом объекте и последствий от их реализации;

в) управление (администрирование) подсистемой безопасности значимого объекта;

г) управление конфигурацией значимого объекта и его подсистемой безопасности;

д) реагирование на компьютерные инциденты в ходе эксплуатации значимого объекта;

е) обеспечение действий в нештатных ситуациях в ходе эксплуатации значимого объекта;

ж) информирование и обучение персонала значимого объекта;

з) контроль за обеспечением безопасности значимого объекта.

13.1. В ходе планирования мероприятий по обеспечению безопасности значимого объекта осуществляются:

а) определение лиц, ответственных за планирование и контроль мероприятий по

обеспечению безопасности значимого объекта;

б) разработка, утверждение и актуализация плана мероприятий по обеспечению безопасности значимого объекта;

в) определения порядка контроля выполнения мероприятий по обеспечению безопасности значимого объекта, предусмотренных утвержденным планом.

Планирование мероприятий по обеспечению безопасности значимого объекта должно осуществляться в рамках процесса планирования, внедренного в соответствии с требованиями к созданию систем безопасности значимых объектов и обеспечению их функционирования, утвержденными в соответствии с пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".

13.2. В ходе анализа угроз безопасности информации в значимом объекте и возможных последствий их реализации осуществляются:

а) анализ уязвимостей значимого объекта, возникающих в ходе его эксплуатации;

б) анализ изменения угроз безопасности информации в значимом объекте, возникающих в ходе его эксплуатации;

в) оценка возможных последствий реализации угроз безопасности информации в значимом объекте.

Периодичность проведения указанных работ определяется субъектом критической информационной инфраструктуры в организационно-распорядительных документах по безопасности значимых объектов с учетом категории значимости объекта и особенностей его функционирования.

13.3. В ходе управления (администрирования) подсистемой безопасности значимого объекта осуществляются:

а) определение лиц, ответственных за управление (администрирование) подсистемой безопасности значимого объекта;

б) управление учетными записями пользователей и поддержание в актуальном состоянии правил разграничения доступа в значимом объекте;

в) управление средствами защиты информации значимого объекта;

г) управление обновлениями программных и программно-аппаратных средств, в том числе средств защиты информации, с учетом особенностей функционирования значимого объекта;

д) централизованное управление подсистемой безопасности значимого объекта (при необходимости);

е) мониторинг и анализ зарегистрированных событий в значимом объекте, связанных с обеспечением безопасности (далее - события безопасности);

ж) сопровождение функционирования подсистемы безопасности значимого объекта в ходе ее эксплуатации, включая ведение эксплуатационной документации и организационно-распорядительных документов по безопасности значимого объекта.

13.4. В ходе управления конфигурацией значимого объекта и его подсистемы безопасности для целей обеспечения его безопасности осуществляются:

а) определение лиц, которым разрешены действия по внесению изменений в конфигурацию значимого объекта и его подсистемы безопасности, и их полномочий;

б) определение компонентов значимого объекта и его подсистемы безопасности, подлежащих изменению в рамках управления конфигурации (идентификация объектов управления конфигурации): программно-аппаратные, программные средства, включая средства защиты информации, и их настройки и программный код, эксплуатационная документация, интерфейсы, файлы и иные компоненты, подлежащие изменению и контролю;

в) управление изменениями значимого объекта и его подсистемы безопасности: разработка параметров настройки, обеспечивающих безопасность значимого объекта, анализ потенциального воздействия планируемых изменений на обеспечение безопасности значимого объекта, санкционирование внесения изменений в значимый объект и его подсистему безопасности, документирование действий по внесению изменений в значимый объект и

сохранение данных об изменениях конфигурации;

г) контроль действий по внесению изменений в значимый объект и его подсистему безопасности.

Реализованные процессы управления изменениями значимого объекта и его подсистемы безопасности должны охватывать процессы гарантийного и (или) технического обслуживания, в том числе дистанционного (удаленного), программных и программно-аппаратных средств, включая средства защиты информации, значимого объекта.

13.5. Реагирование на компьютерные инциденты осуществляется в порядке, установленном в соответствии с пунктом 6 части 4 статьи 6 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".

Для реагирования на компьютерные инциденты определяются работники, ответственные за выявление компьютерных инцидентов и реагирование на них, и определяются их функции.

13.6. Для обеспечения действий в нештатных ситуациях при эксплуатации значимого объекта осуществляются:

а) планирование мероприятий по обеспечению безопасности значимого объекта на случай возникновения нештатных ситуаций;

б) обучение и отработка действий персонала по обеспечению безопасности значимого объекта в случае возникновения нештатных ситуаций;

в) создание альтернативных мест хранения и обработки информации на случай возникновения нештатных ситуаций;

г) резервирование программных и программно-аппаратных средств, в том числе средств защиты информации, каналов связи на случай возникновения нештатных ситуаций;

д) обеспечение возможности восстановления значимого объекта и (или) его компонентов в случае возникновения нештатных ситуаций;

е) определение порядка анализа возникших нештатных ситуаций и принятия мер по недопущению их повторного возникновения.

13.7. В ходе информирования и обучения персонала значимого объекта осуществляются:

а) информирование персонала об угрозах безопасности информации, о правилах безопасной эксплуатации значимого объекта;

б) доведение до персонала требований по обеспечению безопасности значимых объектов, а также положений организационно-распорядительных документов по безопасности значимых объектов в части, их касающейся;

в) обучение персонала правилам эксплуатации отдельных средств защиты информации, включая проведение практических занятий с персоналом;

г) контроль осведомленности персонала об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения безопасности критической информационной инфраструктуры.

Периодичность проведения указанных мероприятий устанавливается субъектом критической информационной инфраструктуры в организационно-распорядительных документах по безопасности значимого объекта с учетом категории значимости и особенностей функционирования значимого объекта.

13.8. В ходе контроля за обеспечением безопасности значимого объекта осуществляются:

а) контроль (анализ) защищенности значимого объекта с учетом особенностей его функционирования;

б) анализ и оценка функционирования значимого объекта и его подсистемы безопасности, включая анализ и устранение уязвимостей и иных недостатков в функционировании подсистемы безопасности значимого объекта;

в) документирование процедур и результатов контроля за обеспечением безопасности значимого объекта;

г) принятие решения по результатам контроля за обеспечением безопасности значимого объекта о необходимости доработки (модернизации) его подсистемы безопасности.

Обеспечение безопасности значимого объекта при выводе его из эксплуатации

14. Обеспечение безопасности значимого объекта при выводе его из эксплуатации или после принятия решения об окончании обработки информации осуществляется субъектом критической информационной инфраструктуры в соответствии с эксплуатационной документацией на значимый объект и организационно-распорядительными документами по безопасности значимого объекта.

Обеспечение безопасности значимого объекта при выводе его из эксплуатации должно предусматривать:

а) архивирование информации, содержащейся в значимом объекте;

б) уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации;

в) уничтожение данных об архитектуре и конфигурации значимого объекта;

г) архивирование или уничтожение эксплуатационной документации на значимый объект и его подсистему безопасности и организационно-распорядительных документов по безопасности значимого объекта.

14.1. Архивирование информации, содержащейся в значимом объекте, должно осуществляться в случае ее дальнейшего использования в деятельности субъекта критической информационной инфраструктуры.

14.2. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации осуществляется в случае обработки значимым объектом информации ограниченного доступа или в случае принятия такого решения субъектом критической информационной инфраструктуры.

Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю значимого объекта или в иные организации для ремонта, технического обслуживания или дальнейшего уничтожения.

При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, производится или физическое уничтожение самих машинных носителей информации или уничтожение содержащейся на машинных носителях информации методами, не предусматривающими возможность ее восстановления.

Уничтожение (стирание) данных и остаточной информации с машинных носителей информации подлежит документированию в соответствии с организационно-распорядительными документами по безопасности значимого объекта.

14.3. При выводе значимого объекта из эксплуатации должен быть осуществлен сброс настроек программных и программно-аппаратных средств, в том числе средств защиты информации, удалена информация о субъектах доступа и объектах доступа, удалены учетные записи пользователей, а также идентификационная и аутентификационная информация субъектов доступа.

14.4. При выводе значимого объекта из эксплуатации вся эксплуатационная документация на значимый объект и его подсистему безопасности, эксплуатационная документация на отдельные средства защиты информации подлежит архивному хранению.

Сроки хранения документации определяются субъектом критической информационной инфраструктуры в организационно-распорядительных документах по безопасности значимого объекта.

По решению субъекта критической информационной инфраструктуры эксплуатационная документация на значимый объект и его подсистему безопасности, а также организационно-распорядительные документы по безопасности значимого объекта (инструкции, руководства) могут быть уничтожены. В этом случае факт уничтожения подлежит документированию

субъектом критической информационной инфраструктуры с указанием наименования, состава документов, способов и даты их уничтожения.

III. Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов

15. Целью обеспечения безопасности значимого объекта является обеспечение его устойчивого функционирования в проектных режимах работы в условиях реализации в отношении значимого объекта угроз безопасности информации.

16. Задачами обеспечения безопасности значимого объекта являются:

а) предотвращение неправомерного доступа к информации, обрабатываемой значимым объектом, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;

б) недопущение информационного воздействия на программные и программно-аппаратные средства, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта;

в) обеспечение функционирования значимого объекта в проектных режимах его работы в условиях воздействия угроз безопасности информации;

г) обеспечение возможности восстановления функционирования значимого объекта критической информационной инфраструктуры.

17. В значимых объектах объектами, подлежащими защите от угроз безопасности информации (объектами защиты), являются:

а) в информационных системах:

информация, обрабатываемая в информационной системе;

программно-аппаратные средства (в том числе машинные носители информации, автоматизированные рабочие места, серверы, телекоммуникационное оборудование, линии связи, средства обработки буквенно-цифровой, графической, видео- и речевой информации);

программные средства (в том числе микропрограммное, общесистемное, прикладное программное обеспечение);

средства защиты информации;

архитектура и конфигурация информационной системы;

б) в информационно-телекоммуникационных сетях:

информация, передаваемая по линиям связи;

телекоммуникационное оборудование (в том числе программное обеспечение, система управления);

средства защиты информации;

архитектура и конфигурация информационно-телекоммуникационной сети;

в) в автоматизированных системах управления:

информация (данные) о параметрах (состоянии) управляемого (контролируемого) объекта или процесса (в том числе входная (выходная) информация, управляющая (командная) информация, контрольно-измерительная информация, иная критически важная (технологическая) информация);

программно-аппаратные средства (в том числе автоматизированные рабочие места, промышленные серверы, телекоммуникационное оборудование, линии связи, программируемые логические контроллеры, производственное, технологическое оборудование (исполнительные устройства);

программные средства (в том числе микропрограммное, общесистемное, прикладное программное обеспечение);

средства защиты информации;

архитектура и конфигурация автоматизированной системы управления.

18. Обеспечение безопасности значимого объекта достигается путем принятия в рамках

подсистемы безопасности значимого объекта совокупности организационных и технических мер, направленных на блокирование (нейтрализацию) угроз безопасности информации, реализация которых может привести к прекращению или нарушению функционирования значимого объекта и обеспечивающего (управляемого, контролируемого) им процесса, а также нарушению безопасности обрабатываемой информации (нарушению доступности, целостности, конфиденциальности информации).

Организационные и технические меры по обеспечению безопасности значимого объекта принимаются субъектом критической информационной инфраструктуры совместно с лицом, эксплуатирующим значимый объект (при его наличии). При этом между субъектом критической информационной инфраструктуры и лицом, эксплуатирующим значимый объект, должно быть проведено разграничение функций по обеспечению безопасности значимого объекта в ходе его эксплуатации.

19. Меры по обеспечению безопасности выбираются и реализуются в значимом объекте с учетом угроз безопасности информации применительно ко всем объектам и субъектам доступа на аппаратном, системном, прикладном и сетевом уровнях, в том числе в среде виртуализации.

20. Меры по обеспечению безопасности значимого объекта принимаются субъектом критической информационной инфраструктуры самостоятельно или при необходимости с привлечением в соответствии с законодательством Российской Федерации организаций, имеющих в зависимости от информации, обрабатываемой значимым объектом, лицензию на деятельность по технической защите информации, составляющей государственную тайну, и (или) на деятельность по технической защите конфиденциальной информации

21. Принимаемые организационные и технические меры по обеспечению безопасности значимого объекта должны соотноситься с мерами по промышленной, функциональной безопасности, иными мерами по обеспечению безопасности значимого объекта и обеспечивающего (управляемого, контролируемого) объекта или процесса. При этом меры по обеспечению безопасности значимого объекта не должны оказывать отрицательного влияния на функционирование значимого объекта в проектных режимах его работы.

22. В значимых объектах в зависимости от их категории значимости и угроз безопасности информации должны быть реализованы следующие организационные и технические меры:

идентификация и аутентификация (ИАФ);

управление доступом (УПД);

ограничение программной среды (ОПС);

защита машинных носителей информации (ЗНИ);

аудит безопасности (АУД);

антивирусная защита (АВЗ);

предотвращение вторжений (компьютерных атак) (СОВ);

обеспечение целостности (ОЦЛ);

обеспечение доступности (ОДТ);

защита технических средств и систем (ЗТС);

защита информационной (автоматизированной) системы и ее компонентов (ЗИС);

планирование мероприятий по обеспечению безопасности (ПЛН);

управление конфигурацией (УКФ);

управление обновлениями программного обеспечения (ОПО);

реагирование на инциденты информационной безопасности (ИНЦ);

обеспечение действий в нештатных ситуациях (ДНС);

информирование и обучение персонала (ИПО).

Состав мер по обеспечению безопасности значимых объектов в зависимости от категории значимости приведен в приложении к настоящим Требованиям.

При реализации мер по обеспечению безопасности значимых объектов применяются методические документы, разработанные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085.

23. Выбор мер по обеспечению безопасности значимых объектов для их реализации включает:

а) определение базового набора мер по обеспечению безопасности значимого объекта;

б) адаптацию базового набора мер по обеспечению безопасности значимого объекта;

в) дополнение адаптированного набора мер по обеспечению безопасности значимого объекта мерами, установленными иными нормативными правовыми актами в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации и защиты информации.

Базовый набор мер по обеспечению безопасности значимого объекта определяется на основе установленной категории значимости значимого объекта в соответствии с приложением к настоящим Требованиям.

Базовый набор мер по обеспечению безопасности значимого объекта подлежит адаптации в соответствии с угрозами безопасности информации, применяемыми информационными технологиями и особенностями функционирования значимого объекта. При этом из базового набора могут быть исключены меры, непосредственно связанные с информационными технологиями, не используемыми в значимом объекте, или характеристиками, не свойственными значимому объекту. При адаптации базового набора мер по обеспечению безопасности значимого объекта для каждой угрозы безопасности информации, включенной в модель угроз, сопоставляется мера или группа мер, обеспечивающие блокирование одной или нескольких угроз безопасности или снижающие возможность ее реализации исходя из условий функционирования значимого объекта. В случае если базовый набор мер не позволяет обеспечить блокирование (нейтрализацию) всех угроз безопасности информации, в него дополнительно включаются меры, приведенные в приложении к настоящим Требованиям.

Дополнение адаптированного набора мер по обеспечению безопасности значимого объекта осуществляется с целью выполнения требований, установленных иными нормативными правовыми актами в области обеспечения безопасности критической информационной инфраструктуры и защиты информации. Дополнение адаптированного набора мер проводится в случае, если в отношении значимого объекта в соответствии с законодательством Российской Федерации также установлены требования о защите информации, содержащейся в государственных информационных системах, требования к защите персональных данных при их обработке в информационных системах персональных данных, требования к криптографической защите информации или иные требования в области защиты информации и обеспечения безопасности критической информационной инфраструктуры.

24. В случае если значимый объект является государственной информационной системой или информационной системой персональных данных, меры по обеспечению безопасности значимого объекта и меры защиты информации (по обеспечению персональных данных) принимаются в соответствии с более высокой категорией значимости, классом защищенности или уровнем защищенности персональных данных.

25. Если принятые в значимом объекте меры по обеспечению промышленной, функциональной безопасности и (или) физической безопасности достаточны для блокирования (нейтрализации) отдельных угроз безопасности информации, дополнительные меры, выбранные в соответствии с пунктами 22 и 23 настоящих Требований, могут не применяться. При этом в ходе разработки организационных и технических мер по обеспечению безопасности значимого объекта должна быть обоснована достаточность применения мер по обеспечению промышленной безопасности или физической безопасности для блокирования (нейтрализации) соответствующих угроз безопасности информации.

26. При отсутствии возможности реализации отдельных мер по обеспечению безопасности и (или) невозможности их применения к отдельным объектам и субъектам доступа, в том числе вследствие их негативного влияния на функционирование значимого объекта в проектных режимах значимого объекта, должны быть разработаны и внедрены компенсирующие меры, обеспечивающие блокирование (нейтрализацию) угроз безопасности информации с

необходимым уровнем защищенности значимого объекта. При этом в ходе разработки организационных и технических мер по обеспечению безопасности значимого объекта должно быть обосновано применение компенсирующих мер, а при приемочных испытаниях (аттестации) оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

В качестве компенсирующих мер могут быть рассмотрены меры по обеспечению промышленной, функциональной и (или) физической безопасности значимого объекта, поддерживающие необходимый уровень его защищенности.

27. Технические меры по обеспечению безопасности в значимом объекте реализуются посредством использования программных и программно-аппаратных средств, применяемых для обеспечения безопасности значимых объектов - средств защиты информации (в том числе встроенных в общесистемное, прикладное программное обеспечение).

При этом в приоритетном порядке подлежат применению средства защиты информации, встроенные в программное обеспечение и (или) программно-аппаратные средства значимых объектов (при их наличии).

28. Для обеспечения безопасности значимых объектов критической информационной инфраструктуры должны применяться средства защиты информации, прошедшие оценку на соответствие требованиям по безопасности в формах обязательной сертификации, испытаний или приемки.

Средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации, применяются в случаях, установленных законодательством Российской Федерации, а также в случае принятия решения субъектом критической информационной инфраструктуры.

В иных случаях применяются средства защиты информации, прошедшие оценку соответствия в форме испытаний или приемки, которые проводятся субъектами критической информационной инфраструктуры самостоятельно или с привлечением организаций, имеющих в соответствии с законодательством Российской Федерации лицензии на деятельность в области защиты информации.

Испытания (приемка) средств защиты информации проводятся отдельно или в составе значимого объекта критической информационной инфраструктуры в соответствии с программой и методиками испытаний (приемки), утверждаемыми субъектом критической информационной инфраструктуры.

29. В случае использования в значимом объекте сертифицированных на соответствие требованиям по безопасности информации средств защиты информации:

а) в значимых объектах 1 категории применяются средства защиты информации не ниже 4 класса защиты, а также средства вычислительной техники не ниже 5 класса;

б) в значимых объектах 2 категории применяются средства защиты информации не ниже 5 класса защиты, а также средства вычислительной техники не ниже 5 класса;

в) в значимых объектах 3 категории применяются средства защиты информации 6 класса защиты, а также средства вычислительной техники не ниже 5 класса.

При этом в значимых объектах 1 и 2 категорий значимости применяются сертифицированные средства защиты информации, прошедшие проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей. Субъектом критической информационной инфраструктуры может быть принято решение о повышении уровня контроля отсутствия недекларированных возможностей средств защиты информации.

Классы защиты определяются в соответствии с нормативными правовыми актами ФСТЭК России, изданными в соответствии с подпунктом 13.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085.

При использовании в значимом объекте средств защиты информации, сертифицированных по требованиям безопасности информации, указанные средства должны быть сертифицированы на соответствие обязательным требованиям по безопасности информации, установленным

нормативными правовыми актами, или требованиям, указанным в технических условиях (заданиях по безопасности).

Функции безопасности средств защиты информации должны обеспечивать выполнение настоящих Требований.

30. Применяемые в значимом объекте программные и программно-аппаратные средства, в том числе средства защиты информации, должны эксплуатироваться в соответствии с инструкциями (правилами) по эксплуатации, разработанными разработчиками (производителями) этих средств, и иной эксплуатационной документацией.

31. Применяемые в значимом объекте программные и программно-аппаратные средства, в том числе средства защиты информации, должны быть обеспечены гарантийной и (или) технической поддержкой.

При выборе программных и программно-аппаратных средств, в том числе средств защиты информации, необходимо учитывать наличие ограничений на возможность их применения субъектом критической информационной инфраструктуры на любом из принадлежащих ему значимых объектов критической информационной инфраструктуры со стороны разработчиков (производителей) или иных лиц.

В значимом объекте не допускаются:

наличие удаленного доступа непосредственно (напрямую) к программным и программно-аппаратным средствам, в том числе средствам защиты информации, для обновления или управления со стороны лиц, не являющихся работниками субъекта критической информационной инфраструктуры;

наличие локального бесконтрольного доступа к программным и программно-аппаратным средствам, в том числе средствам защиты информации, для обновления или управления со стороны лиц, не являющихся работниками субъекта критической информационной инфраструктуры;

передача информации, в том числе технологической информации, разработчику (производителю) программных и программно-аппаратных средств, в том числе средств защиты информации, или иным лицам без контроля со стороны субъекта критической информационной инфраструктуры.

32. При использовании в значимых объектах новых информационных технологий и выявлении дополнительных угроз безопасности информации, для которых не определены меры по обеспечению безопасности, должны разрабатываться компенсирующие меры в соответствии с пунктом 26 настоящих Требований.

Приложение
к Требованиям по обеспечению
безопасности значимых объектов
критической информационной
инфраструктуры Российской Федерации,
утвержденным приказом ФСТЭК России
от 25 декабря 2017 г. N 239

СОСТАВ
МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ДЛЯ ЗНАЧИМОГО ОБЪЕКТА СООТВЕТСТВУЮЩЕЙ КАТЕГОРИИ ЗНАЧИМОСТИ

Обозначение и номер меры	**Меры обеспечения безопасности значимого объекта**	**Категория значимости**		
		3	**2**	**1**
I. Идентификация и аутентификация (ИАФ)				
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	+	+	+
II. Управление доступом (УПД)				
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	+	+	+
III. Ограничение программной среды (ОПС)				
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			
IV. Защита машинных носителей информации (ЗНИ)				
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			
V. Аудит безопасности (АУД)				
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			+
VI. Антивирусная защита (АВЗ)				
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			+
VII. Предотвращение вторжений (компьютерных атак) (СОВ)				
СОВ.0	Разработка политики предотвращения вторжений (компьютерных атак)		+	+
СОВ.1	Обнаружение и предотвращение компьютерных атак		+	+
СОВ.2	Обновление базы решающих правил		+	+
VIII. Обеспечение целостности (ОЦЛ)				

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			
IX. Обеспечение доступности (ОДТ)				
ОДТ.0	Разработка политики обеспечения доступности	+	+	+
ОДТ.1	Использование отказоустойчивых технических средств		+	+
0ДТ.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	+	+	+
X. Защита технических средств и систем (ЗТС)				
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			
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)				
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			
XII. Реагирование на компьютерные инциденты (ИНЦ)				
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)				
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. Управление обновлениями программного обеспечения (ОПО)				
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	+	+	+
XV. Планирование мероприятий по обеспечению безопасности (ПЛН)				
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	+	+	+
XVI. Обеспечение действий в нештатных ситуациях (ДНС)				
ДНС.0	Разработка политики обеспечения действий в нештатных 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 ситуаций		+	+
ДНС.4	Резервирование программного обеспечения, технических средств, каналов связи на случай возникновения нештатных ситуаций		+	+
ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций	+		+
ДНС.6	Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения	+	+	+
XVII. Информирование и обучение персонала (ИПО)				
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	+	+	+

"+" - мера обеспечения безопасности включена в базовый набор мер для соответствующей категории значимого объекта.

Меры обеспечения безопасности, не обозначенные знаком "+", применяются при адаптации и дополнении базового набора мер, а также при разработке компенсирующих мер в значимом объекте критической информационной инфраструктуры соответствующей категории значимости.

Зарегистрировано в Минюсте России 30 июня 2014 г. N 32919

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ПРИКАЗ
от 14 марта 2014 г. N 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

(в ред. Приказов ФСТЭК России от 23.03.2017 N 49, от 09.08.2018 N 138)

В соответствии с Положением о Федеральной службе по техническому и экспортному контролю, утвержденным Указом Президента Российской Федерации от 16 августа 2004 г. N 1085 (Собрание законодательства Российской Федерации, 2004, N 34, ст. 3541; 2006, N 49, ст. 5192; 2008, N 43, ст. 4921; N 47, ст. 5431; 2012, N 7, ст. 818; 2013, N 26, ст. 3314; N 52, ст. 7137), приказываю:

Утвердить прилагаемые Требования 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.

Директор
Федеральной службы по техническому и
экспортному контролю В.СЕЛИН

Утверждены
приказом ФСТЭК России
от 14 марта 2014 г. N 31

ТРЕБОВАНИЯ 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

(в ред. Приказов ФСТЭК России от 23.03.2017 N 49, от 09.08.2018 N 138)

I. Общие положения

1. В настоящем документе устанавливаются 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.

Обеспечение безопасности автоматизированных систем управления, являющихся значимыми объектами критической информационной инфраструктуры Российской Федерации, осуществляется в соответствии с Требованиями по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденными приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. N 239, а также Требованиями к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденными приказом Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 г. N 235 (зарегистрирован Минюстом России 22 февраля 2018 г., регистрационный N 50118).

Настоящие Требования применяются в случае принятия владельцем автоматизированной системы управления решения об обеспечении защиты информации, обработка которой осуществляется этой системой и нарушение безопасности которой может привести к нарушению функционирования автоматизированной системы управления.

В случае необходимости применение криптографических методов защиты информации и шифровальных (криптографических) средств защиты информации осуществляется в соответствии с законодательством Российской Федерации.

2. Настоящие Требования направлены на обеспечение функционирования автоматизированной системы управления в штатном режиме, при котором обеспечивается соблюдение проектных пределов значений параметров выполнения целевых функций автоматизированной системы управления в условиях воздействия угроз безопасности информации, а также на снижение рисков незаконного вмешательства в процессы функционирования автоматизированных систем управления критически важных объектов, потенциально опасных объектов, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, в том числе опасных производственных объектов (далее - управляемые (контролируемые) объекты), безопасность которых обеспечивается в соответствии с законодательством Российской Федерации о безопасности

объектов топливно-энергетического комплекса, о транспортной безопасности, об использовании атомной энергии, о промышленной безопасности опасных производственных объектов, о безопасности гидротехнических сооружений и иных законодательных актов Российской Федерации.

3. Действие настоящих требований распространяется на автоматизированные системы управления, обеспечивающие контроль и управление технологическим и (или) производственным оборудованием (исполнительными устройствами) и реализованными на нем технологическими и (или) производственными процессами (в том числе системы диспетчерского управления, системы сбора (передачи) данных, системы, построенные на основе программируемых логических контроллеров, распределенные системы управления, системы управления станками с числовым программным управлением).

4. Настоящие Требования предназначены для лиц, устанавливающих требования к защите информации в автоматизированных системах управления (далее - заказчик), лиц, обеспечивающих эксплуатацию автоматизированных систем управления (далее - оператор), а также лиц, привлекаемых в соответствии с законодательством Российской Федерации к проведению работ по созданию (проектированию) автоматизированных систем управления и (или) их систем защиты (далее - разработчик).

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

6. Защита информации в автоматизированной системе управления обеспечивается путем выполнения заказчиком, оператором и разработчиком требований к организации защиты информации в автоматизированной системе управления и требований к мерам защиты информации в автоматизированной системе управления.

II. Требования к организации защиты информации в автоматизированной системе управления

7. Автоматизированная система управления, как правило, имеет многоуровневую структуру:

уровень операторского (диспетчерского) управления (верхний уровень);

уровень автоматического управления (средний уровень);

уровень ввода (вывода) данных исполнительных устройств (нижний (полевой) уровень).

Автоматизированная система управления может включать:

а) на уровне операторского (диспетчерского) управления:

операторские (диспетчерские), инженерные автоматизированные рабочие места, промышленные серверы (SCADA-серверы) с установленным на них общесистемным и прикладным программным обеспечением, телекоммуникационное оборудование (коммутаторы, маршрутизаторы, межсетевые экраны, иное оборудование), а также каналы связи;

б) на уровне автоматического управления:

программируемые логические контроллеры, иные технические средства с установленным программным обеспечением, получающие данные с нижнего (полевого) уровня, передающие данные на верхний уровень для принятия решения по управлению объектом и (или) процессом и формирующие управляющие команды (управляющую (командную) информацию) для исполнительных устройств, а также промышленная сеть передачи данных;

в) на уровне ввода (вывода) данных (исполнительных устройств):

датчики, исполнительные механизмы, иные аппаратные устройства с установленными в них микропрограммами и машинными контроллерами.

Количество уровней автоматизированной системы управления и ее состав на каждом из уровней зависит от назначения автоматизированной системы управления и выполняемых ею целевых функций. На каждом уровне автоматизированной системы управления по функциональным, территориальным или иным признакам могут выделяться дополнительные

сегменты.

В автоматизированной системе управления объектами защиты являются:

информация (данные) о параметрах (состоянии) управляемого (контролируемого) объекта или процесса (входная (выходная) информация, управляющая (командная) информация, контрольно-измерительная информация, иная критически важная (технологическая) информация);

программно-технический комплекс, включающий технические средства (в том числе автоматизированные рабочие места, промышленные серверы, телекоммуникационное оборудование, каналы связи, программируемые логические контроллеры, исполнительные устройства), программное обеспечение (в том числе микропрограммное, общесистемное, прикладное), а также средства защиты информации.

8. Защита информации в автоматизированной системе управления является составной частью работ по созданию (модернизации) и эксплуатации автоматизированной системы управления и обеспечивается на всех стадиях (этапах) ее создания и в ходе эксплуатации.

Защита информации в автоматизированной системе управления достигается путем принятия в рамках системы защиты автоматизированной системы управления совокупности организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации, реализация которых может привести к нарушению штатного режима функционирования автоматизированной системы управления и управляемого (контролируемого) объекта и (или) процесса, на локализацию и минимизацию последствий от возможной реализации угроз безопасности информации, восстановление штатного режима функционирования автоматизированной системы управления в случае реализации угроз безопасности информации.

Принимаемые организационные и технические меры защиты информации:

должны обеспечивать доступность обрабатываемой в автоматизированной системе управления информации (исключение неправомерного блокирования информации), ее целостность (исключение неправомерного уничтожения, модифицирования информации), а также, при необходимости, конфиденциальность (исключение неправомерного доступа, копирования, предоставления или распространения информации);

должны соотноситься с мерами по промышленной, физической, пожарной, экологической, радиационной безопасности, иными мерами по обеспечению безопасности автоматизированной системы управления и управляемого (контролируемого) объекта и (или) процесса;

не должны оказывать отрицательного влияния на штатный режим функционирования автоматизированной системы управления.

9. Проведение работ по защите информации в соответствии с настоящими Требованиями в ходе создания (модернизации) и эксплуатации автоматизированной системы управления осуществляется заказчиком, оператором и (или) разработчиком самостоятельно и (или) при необходимости с привлечением в соответствии с законодательством Российской Федерации организаций, имеющих лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 4 мая 2011 г. N 99-ФЗ "О лицензировании отдельных видов деятельности" (Собрание законодательства Российской Федерации, 2011, N 19, ст. 2716; N 30, ст. 4590; N 43, ст. 5971; N 48, ст. 6728; 2012, N 26, ст. 3446; N 31, ст. 4322; 2013, N 9, ст. 874; N 27, ст. 3477).

10. Для обеспечения защиты информации в автоматизированной системе управления оператором назначается структурное подразделение или должностное лицо (работник), ответственные за защиту информации.

11. В автоматизированной системе управления применяются средства защиты информации, прошедшие оценку соответствия в соответствии с законодательством Российской Федерации о техническом регулировании.

12. Для обеспечения защиты информации в автоматизированной системе управления проводятся следующие мероприятия:

формирование требований к защите информации в автоматизированной системе

управления;

разработка системы защиты автоматизированной системы управления;

внедрение системы защиты автоматизированной системы управления и ввод ее в действие;

обеспечение защиты информации в ходе эксплуатации автоматизированной системы управления;

обеспечение защиты информации при выводе из эксплуатации автоматизированной системы управления.

Формирование требований к защите информации в автоматизированной системе управления

13. Формирование требований к защите информации в автоматизированной системе управления осуществляется заказчиком.

Формирование требований к защите информации в автоматизированной системе управления осуществляется с учетом ГОСТ Р 51583 "Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения" (далее - ГОСТ Р 51583), ГОСТ Р 51624 "Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования" (далее - ГОСТ Р 51624) и стандартов организации и в том числе включает:

принятие решения о необходимости защиты информации в автоматизированной системе управления;

классификацию автоматизированной системы управления по требованиям защиты информации (далее - классификация автоматизированной системы управления);

определение угроз безопасности информации, реализация которых может привести к нарушению штатного режима функционирования автоматизированной системы управления, и разработку на их основе модели угроз безопасности информации;

определение требований к системе защиты автоматизированной системы управления.

13.1. При принятии решения о необходимости защиты информации в автоматизированной системе управления осуществляются:

анализ целей создания автоматизированной системы управления и задач, решаемых этой автоматизированной системой управления;

определение информации, нарушение доступности, целостности или конфиденциальности которой может привести к нарушению штатного режима функционирования автоматизированной системы управления (определение критически важной информации), и оценка возможных последствий такого нарушения;

анализ нормативных правовых актов, локальных правовых актов, методических документов, национальных стандартов и стандартов организаций, которым должна соответствовать автоматизированная система управления;

принятие решения о необходимости создания системы защиты автоматизированной системы управления и определение целей и задач защиты информации в автоматизированной системе управления.

13.2. Классификация автоматизированной системы управления проводится заказчиком или оператором в зависимости от уровня значимости (критичности) информации, обработка которой осуществляется в автоматизированной системе управления.

Устанавливаются три класса защищенности автоматизированной системы управления, определяющие уровни защищенности автоматизированной системы управления. Самый низкий класс - третий, самый высокий - первый. Класс защищенности автоматизированной системы управления определяется в соответствии с приложением N 1 к настоящим Требованиям.

Класс защищенности может быть установлен отдельно для каждого из уровней автоматизированной системы управления или иных сегментов при их наличии.

Результаты классификации автоматизированной системы управления оформляются актом

классификации.

Требование к классу защищенности включается в техническое задание на создание автоматизированной системы управления и (или) техническое задание (частное техническое задание) на создание системы защиты автоматизированной системы управления, разрабатываемые с учетом ГОСТ 34.602 "Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы" (далее - ГОСТ 34.602), ГОСТ Р 51583, ГОСТ Р 51624 и стандартов организации.

Класс защищенности автоматизированной системы управления (сегмента) подлежит пересмотру только в случае ее модернизации, в результате которой изменился уровень значимости (критичности) информации, обрабатываемой в автоматизированной системе управления (сегменте).

13.3. Определение угроз безопасности информации осуществляется на каждом из уровней автоматизированной системы управления и должно включать:

а) выявление источников угроз безопасности информации и оценку возможностей (потенциала) внешних и внутренних нарушителей;

б) анализ возможных уязвимостей автоматизированной системы и входящих в ее состав программных и программно-аппаратных средств;

в) определение возможных способов (сценариев) реализации (возникновения) угроз безопасности информации;

г) оценку возможных последствий от реализации (возникновения) угроз безопасности информации, нарушения отдельных свойств безопасности информации (целостности, доступности, конфиденциальности) и автоматизированной системы управления в целом.

В качестве исходных данных при определении угроз безопасности информации используется банк данных угроз безопасности информации, ведение которого осуществляется ФСТЭК России в соответствии с подпунктом 21 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085 (Собрание законодательства Российской Федерации, 2004, N 34, ст. 3541; 2006, N 49, ст. 5192; 2008, N 43, ст. 4921; N 47, ст. 5431; 2012, N 7, ст. 818; 2013, N 26, ст. 3314; N 52, ст. 7137; 2014, N 36, ст. 4833; N 44, ст. 6041; N 4, ст. 641; 2016, N 1, ст. 211; 2017, N 48, ст. 7198; 2018, N 20, ст. 2818), а также иные источники, содержащие сведения об уязвимостях и угрозах безопасности информации.

При определении угроз безопасности информации учитываются структурно-функциональные характеристики автоматизированной системы управления, включающие наличие уровней (сегментов) автоматизированной системы управления, состав автоматизированной системы управления, физические, логические, функциональные и технологические взаимосвязи в автоматизированной системе управления, взаимодействие с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями, режимы функционирования автоматизированной системы управления, а также иные особенности ее построения и функционирования.

По результатам определения угроз безопасности информации могут разрабатываться рекомендации по корректировке структурно-функциональных характеристик автоматизированной системы управления, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

Модель угроз безопасности информации должна содержать описание автоматизированной системы управления и угроз безопасности информации для каждого из уровней автоматизированной системы управления, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей автоматизированной системы управления, способов (сценариев) реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (доступности, целостности, конфиденциальности) и штатного режима функционирования автоматизированной системы управления <*>.

<*> Разработанные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о

Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085 (Собрание законодательства Российской Федерации, 2004, N 34, ст. 3541; 2006, N 49, ст. 5192; 2008, N 43, ст. 4921; N 47, ст. 5431; 2012, N 7, ст. 818; 2013, N 26, ст. 3314; N 52, ст. 7137).

Для определения угроз безопасности информации и разработки модели угроз безопасности информации применяются методические документы ФСТЭК России <*>.

<*> Разработанные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085 (Собрание законодательства Российской Федерации, 2004, N 34, ст. 3541; 2006, N 49, ст. 5192; 2008, N 43, ст. 4921; N 47, ст. 5431; 2012, N 7, ст. 818; 2013, N 26, ст. 3314; N 52, ст. 7137).

13.4. Требования к системе защиты автоматизированной системы управления определяются в зависимости от класса защищенности автоматизированной системы управления и угроз безопасности информации, включенных в модель угроз безопасности информации.

Требования к системе защиты автоматизированной системы управления включаются в техническое задание на создание (модернизацию) автоматизированной системы управления и (или) техническое задание (частное техническое задание) на создание системы защиты автоматизированной системы управления, разрабатываемые с учетом ГОСТ 34.602, ГОСТ Р 51583, ГОСТ Р 51624 и стандартов организации, которые должны в том числе содержать:

цель и задачи обеспечения защиты информации в автоматизированной системе управления;

класс защищенности автоматизированной системы управления;

перечень нормативных правовых актов, локальных правовых актов, методических документов, национальных стандартов и стандартов организаций, которым должна соответствовать автоматизированная система управления;

объекты защиты автоматизированной системы управления на каждом из ее уровней;

требования к мерам и средствам защиты информации, применяемым в автоматизированной системе управления;

требования к защите информации при информационном взаимодействии с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями;

требования к поставляемым техническим средствам, программному обеспечению, средствам защиты информации;

функции заказчика и оператора по обеспечению защиты информации в автоматизированной системе управления;

стадии (этапы работ) создания системы защиты автоматизированной системы управления.

При определении требований к системе защиты автоматизированной системы управления учитываются положения политик обеспечения информационной безопасности заказчика в случае их разработки по ГОСТ Р ИСО/МЭК 27001 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования", а также политик обеспечения информационной безопасности оператора в части, не противоречащей политикам заказчика.

Разработка системы защиты автоматизированной системы управления

14. Разработка системы защиты автоматизированной системы управления организуется заказчиком и осуществляется разработчиком и (или) оператором.

Разработка системы защиты автоматизированной системы управления осуществляется в

соответствии с техническим заданием на создание (модернизацию) автоматизированной системы управления и (или) техническим заданием (частным техническим заданием) на создание системы защиты автоматизированной системы управления с учетом ГОСТ 34.601 "Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания" (далее - ГОСТ 34.601), ГОСТ Р 51583, ГОСТ Р 51624 и стандартов организации и в том числе включает:

проектирование системы защиты автоматизированной системы управления;

разработку эксплуатационной документации на систему защиты автоматизированной системы управления.

Система защиты автоматизированной системы управления не должна препятствовать штатному режиму функционирования автоматизированной системы управления при выполнении ее функций в соответствии с назначением автоматизированной системы управления.

При разработке системы защиты автоматизированной системы управления учитывается ее информационное взаимодействие с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями.

14.1. При проектировании системы защиты автоматизированной системы управления:

определяются типы субъектов доступа (пользователи, процессы и иные субъекты доступа) и объектов доступа, являющихся объектами защиты (автоматизированные рабочие места, промышленные серверы, телекоммуникационное оборудование, программируемые логические контроллеры, исполнительные устройства, иные объекты доступа);

определяются методы управления доступом (дискреционный, мандатный, ролевой или иные методы), типы доступа (чтение, запись, выполнение или иные типы доступа) и правила разграничения доступа субъектов доступа к объектам доступа (на основе списков, меток безопасности, ролей и иных правил), подлежащие реализации в автоматизированной системе управления;

выбираются меры защиты информации, подлежащие реализации в рамках системы защиты автоматизированной системы управления;

определяются параметры программирования и настройки программного обеспечения, включая программное обеспечение средств защиты информации, обеспечивающие реализацию мер защиты информации, а также устранение возможных уязвимостей автоматизированной системы управления;

определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации;

определяется структура системы защиты автоматизированной системы управления, включая состав (количество) и места размещения ее элементов;

осуществляется при необходимости выбор средств защиты информации с учетом их стоимости, совместимости с программным обеспечением и техническими средствами, функций безопасности этих средств и особенностей их реализации, а также класса защищенности автоматизированной системы управления;

определяются меры защиты информации при информационном взаимодействии с иными автоматизированными (информационными) системами и информационно-телекоммуникационными сетями;

осуществляется проверка, в том числе при необходимости с использованием макетов или тестовой зоны, корректности функционирования автоматизированной системы управления с системой защиты и совместимости выбранных средств защиты информации с программным обеспечением и техническими средствами автоматизированной системы управления.

При проектировании системы защиты автоматизированной системы управления должны учитываться особенности функционирования программного обеспечения и технических средств на каждом из уровней автоматизированной системы управления.

Результаты проектирования системы защиты автоматизированной системы управления отражаются в проектной документации (эскизном (техническом) проекте и (или) в рабочей

документации) на автоматизированную систему управления (систему защиты автоматизированной системы управления), разрабатываемой с учетом ГОСТ 34.201 "Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем" (далее - ГОСТ 34.201) и стандартов организации.

14.2. Разработка эксплуатационной документации на систему защиты автоматизированной системы управления осуществляется по результатам проектирования в соответствии с техническим заданием на создание (модернизацию) автоматизированной системы управления и (или) техническим заданием (частным техническим заданием) на создание системы защиты автоматизированной системы управления.

Эксплуатационная документация на систему защиты автоматизированной системы управления разрабатывается с учетом ГОСТ 34.601, ГОСТ 34.201, ГОСТ Р 51624 и стандартов организации и должна в том числе содержать описание:

структуры системы защиты автоматизированной системы управления;

состава, мест установки, параметров и порядка настройки средств защиты информации, программного обеспечения и технических средств;

правил эксплуатации системы защиты автоматизированной системы управления.

Внедрение системы защиты автоматизированной системы управления и ввод ее в действие

15. Внедрение системы защиты автоматизированной системы управления организуется заказчиком и осуществляется разработчиком и (или) оператором.

Внедрение системы защиты автоматизированной системы управления осуществляется в соответствии с проектной и эксплуатационной документацией на систему защиты информации автоматизированной системы управления и в том числе включает:

настройку (задание параметров программирования) программного обеспечения автоматизированной системы управления;

разработку документов, определяющих правила и процедуры (политики), реализуемые оператором для обеспечения защиты информации в автоматизированной системе управления в ходе ее эксплуатации (далее - организационно-распорядительные документы по защите информации);

внедрение организационных мер защиты информации;

установку и настройку средств защиты информации в автоматизированной системе управления;

предварительные испытания системы защиты автоматизированной системы управления;

опытную эксплуатацию системы защиты автоматизированной системы управления;

анализ уязвимостей автоматизированной системы управления и принятие мер по их устранению;

приемочные испытания системы защиты автоматизированной системы управления.

15.1. Настройка (задание параметров программирования) программного обеспечения автоматизированной системы управления должна осуществляться в соответствии с проектной и эксплуатационной документацией на автоматизированную систему управления и обеспечивать конфигурацию программного обеспечения и автоматизированной системы в целом, при которой минимизируются риски возникновения уязвимостей и возможности реализации угроз безопасности информации.

15.2. Разрабатываемые организационно-распорядительные документы по защите информации должны определять правила и процедуры (политики):

реализаций отдельных мер защиты информации в автоматизированной системе управления в рамках ее системы защиты;

планирования мероприятий по обеспечению защиты информации в автоматизированной системе управления;

обеспечения действий в нештатных (непредвиденных) ситуациях в ходе эксплуатации автоматизированной системы управления;

информирования и обучения персонала автоматизированной системы управления;

анализа угроз безопасности информации в автоматизированной системе управления и рисков от их реализации;

управления (администрирования) системой защиты информации автоматизированной системы управления;

выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования автоматизированной системы управления и (или) к возникновению угроз безопасности информации (далее - инциденты), и реагирования на них;

управления конфигурацией автоматизированной системы управления и ее системы защиты;

контроля (мониторинга) за обеспечением уровня защищенности автоматизированной системы управления;

защиты информации при выводе из эксплуатации автоматизированной системы управления.

Организационно-распорядительные документы по защите информации могут разрабатываться в виде отдельных документов оператора или в рамках общей политики обеспечения информационной безопасности в случае ее разработки по ГОСТ Р ИСО/МЭК 27001 "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования".

15.3. При внедрении организационных мер защиты информации осуществляются:

введение ограничений на действия персонала (пользователей (операторского персонала), администраторов, обеспечивающего персонала), а также на условия эксплуатации, изменение состава и конфигурации технических средств и программного обеспечения;

определение администратора безопасности информации;

реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа;

проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий персонала автоматизированной системы управления и администратора безопасности информации, направленных на обеспечение защиты информации;

отработка практических действий должностных лиц и подразделений, обеспечивающих эксплуатацию автоматизированной системы управления и защиту информации.

15.4. Установка и настройка средств защиты информации осуществляется в случаях, если такие средства необходимы для блокирования (нейтрализации) угроз безопасности информации, которые невозможно исключить настройкой (заданием параметров) программного обеспечения автоматизированной системы управления и (или) реализацией организационных мер защиты информации.

Установка и настройка средств защиты информации в автоматизированной системе управления должна проводиться в соответствии с эксплуатационной документацией на систему защиты автоматизированной системы управления и документацией на средства защиты информации.

При этом установка и настройка средств защиты информации должна обеспечивать корректность функционирования автоматизированной системы управления и совместимость выбранных средств защиты информации с программным обеспечением и техническими средствами автоматизированной системы управления. Установленные и настроенные средства защиты информации не должны оказывать отрицательного влияния на штатный режим функционирования автоматизированной системы управления.

15.5. Предварительные испытания системы защиты автоматизированной системы управления проводятся с учетом ГОСТ 34.603 "Информационная технология. Виды испытаний автоматизированных систем" (далее - ГОСТ 34.603) и стандартов организации и включают

проверку работоспособности системы защиты автоматизированной системы управления, а также принятие решения о возможности опытной эксплуатации системы защиты автоматизированной системы управления.

По результатам предварительных испытаний системы защиты автоматизированной системы управления могут разрабатываться предложения по корректировке проектных решений по автоматизированной системе управления и (или) ее системе защиты.

15.6. Опытная эксплуатация системы защиты автоматизированной системы управления проводится с учетом ГОСТ 34.603 и стандартов организации и включает проверку функционирования системы защиты автоматизированной системы управления, в том числе реализованных мер защиты информации, а также готовность персонала автоматизированной системы управления к эксплуатации системы защиты автоматизированной системы управления.

По результатам опытной эксплуатации системы защиты автоматизированной системы управления могут разрабатываться предложения по корректировке проектных решений по автоматизированной системе управления и (или) ее системе защиты.

15.7. Анализ уязвимостей автоматизированной системы управления проводится в целях оценки возможности преодоления нарушителем системы защиты автоматизированной системы управления и нарушения безопасного функционирования автоматизированной системы управления за счет реализации угроз безопасности информации.

Анализ уязвимостей автоматизированной системы управления включает анализ уязвимостей средств защиты информации, технических средств и программного обеспечения автоматизированной системы управления.

При анализе уязвимостей автоматизированной системы управления проверяется отсутствие уязвимостей средств защиты информации, технических средств и программного обеспечения, в том числе с учетом информации, имеющейся у разработчиков и полученной из других общедоступных источников, правильность установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректность работы средств защиты информации, технических средств и программного обеспечения автоматизированной системы управления при их взаимодействии.

По решению заказчика для подтверждения выявленных уязвимостей может проводиться тестирование автоматизированной системы управления на проникновение. Указанное тестирование проводится, как правило, на макете (в тестовой зоне) автоматизированной системы управления.

В случае выявления уязвимостей в автоматизированной системе управления, приводящих к возникновению дополнительных угроз безопасности информации, проводится уточнение модели угроз безопасности информации и при необходимости принимаются дополнительные меры защиты информации, направленные на устранение выявленных уязвимостей или исключающие возможность эксплуатации нарушителем выявленных уязвимостей.

Анализ уязвимостей автоматизированной системы управления проводится до ввода автоматизированной системы управления в промышленную эксплуатацию на этапах, определяемых заказчиком.

15.8. Приемочные испытания системы защиты автоматизированной системы управления проводятся, как правило, в рамках приемочных испытаний автоматизированной системы управления в целом с учетом ГОСТ 34.603 и стандартов организации.

В ходе приемочных испытаний должен быть проведен комплекс организационных и технических мероприятий (испытаний), в результате которых подтверждается соответствие системы защиты автоматизированной системы управления техническому заданию на создание (модернизацию) автоматизированной системы управления и (или) техническому заданию (частному техническому заданию) на создание системы защиты автоматизированной системы управления, а также настоящим Требованиям.

В качестве исходных данных при приемочных испытаниях используются модель угроз безопасности информации, акт классификации автоматизированной системы управления,

техническое задание на создание (модернизацию) автоматизированной системы управления и (или) техническое задание (частное техническое задание) на создание системы защиты автоматизированной системы управления, проектная и эксплуатационная документация на систему защиты автоматизированной системы управления, организационно-распорядительные документы по защите информации, результаты анализа уязвимостей автоматизированной системы управления, материалы предварительных и приемочных испытаний системы защиты автоматизированной системы управления, а также иные документы, разрабатываемые в соответствии с настоящими Требованиями и требованиями стандартов организации.

Приемочные испытания системы защиты автоматизированной системы управления проводятся в соответствии с программой и методикой приемочных испытаний. Результаты приемочных испытаний системы защиты автоматизированной системы управления с выводом о ее соответствии установленным требованиям включаются в акт приемки автоматизированной системы управления в эксплуатацию.

По решению заказчика подтверждение соответствия системы защиты автоматизированной системы управления техническому заданию на создание (модернизацию) автоматизированной системы управления и (или) техническому заданию (частному техническому заданию) на создание системы защиты автоматизированной системы управления, а также настоящим Требованиям может проводиться в форме аттестации автоматизированной системы управления на соответствие требованиям по защите информации. В этом случае для проведения аттестации применяются национальные стандарты, а также методические документы ФСТЭК России <*>.

<*> Разработанные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085.

Ввод в действие автоматизированной системы управления осуществляется с учетом ГОСТ 34.601, стандартов организации и при положительном заключении (выводе) в акте приемки о соответствии ее системы защиты установленным требованиям к защите информации (или при наличии аттестата соответствия).

Обеспечение защиты информации в ходе эксплуатации автоматизированной системы управления

16. Обеспечение защиты информации в ходе эксплуатации автоматизированной системы управления осуществляется оператором в соответствии с эксплуатационной документацией на систему защиты и организационно-распорядительными документами по защите информации и включает следующие процедуры:

планирование мероприятий по обеспечению защиты информации в автоматизированной системе управления;

обеспечение действий в нештатных (непредвиденных) ситуациях в ходе эксплуатации автоматизированной системы управления;

информирование и обучение персонала автоматизированной системы управления;

периодический анализ угроз безопасности информации в автоматизированной системе управления и рисков от их реализации;

управление (администрирование) системой защиты автоматизированной системы управления;

выявление инцидентов в ходе эксплуатации автоматизированной системы управления и реагирование на них;

управление конфигурацией автоматизированной системы управления и ее системы защиты;

контроль (мониторинг) за обеспечением уровня защищенности автоматизированной системы управления.

16.1. В ходе планирования мероприятий по обеспечению защиты информации в автоматизированной системе управления осуществляются:

определение лиц, ответственных за планирование и контроль мероприятий по обеспечению защиты информации в автоматизированной системе управления;

разработка, утверждение и актуализация плана мероприятий по обеспечению защиты информации в автоматизированной системе управления;

контроль выполнения мероприятий по обеспечению защиты информации в автоматизированной системе управления, предусмотренных утвержденным планом.

16.2. В ходе обеспечения действий в нештатных (непредвиденных) ситуациях при эксплуатации автоматизированной системы управления осуществляются:

планирование мероприятий по обеспечению защиты информации в автоматизированной системе управления на случай возникновения нештатных (непредвиденных) ситуаций;

обучение и отработка действий персонала по обеспечению защиты информации в автоматизированной системе управления в случае возникновения нештатных (непредвиденных) ситуаций;

создание альтернативных мест хранения и обработки информации на случай возникновения нештатных (непредвиденных) ситуаций;

резервирование программного обеспечения, технических средств, каналов передачи данных автоматизированной системы управления на случай возникновения нештатных (непредвиденных) ситуаций;

обеспечение возможности восстановления автоматизированной системы управления и (или) ее компонентов в случае возникновения нештатных (непредвиденных) ситуаций.

16.3. В ходе информирования и обучения персонала автоматизированной системы управления осуществляются:

периодическое информирование персонала об угрозах безопасности информации, о правилах эксплуатации системы защиты автоматизированной системы управления и отдельных средств защиты информации;

периодическое обучение персонала правилам эксплуатации системы защиты автоматизированной системы управления и отдельных средств защиты информации, включая проведение практических занятий с персоналом на макетах или в тестовой зоне.

16.4. В ходе анализа угроз безопасности информации в автоматизированной системе управления и возможных рисков от их реализации осуществляются:

периодический анализ уязвимостей автоматизированной системы управления, возникающих в ходе ее эксплуатации;

периодический анализ изменения угроз безопасности информации в автоматизированной системе управления, возникающих в ходе ее эксплуатации;

периодическая оценка последствий от реализации угроз безопасности информации в автоматизированной системе управления (анализ риска).

16.5. В ходе управления (администрирования) системой защиты автоматизированной системы управления осуществляются:

определение лиц, ответственных за управление (администрирование) системой защиты автоматизированной системы управления;

управление учетными записями пользователей и поддержание правил разграничения доступа в автоматизированной системе управления в актуальном состоянии;

управление средствами защиты информации в автоматизированной системе управления, в том числе параметрами настройки программного обеспечения, включая восстановление работоспособности средств защиты информации, генерацию, смену и восстановление паролей;

управление обновлениями программного обеспечения, включая программное обеспечение средств защиты информации, с учетом особенностей функционирования автоматизированной системы управления;

централизованное управление системой защиты автоматизированной системы управления (при необходимости);

анализ зарегистрированных событий в автоматизированной системе управления, связанных с безопасностью информации (далее - события безопасности);

сопровождение функционирования системы защиты автоматизированной системы управления в ходе ее эксплуатации, включая ведение эксплуатационной документации и организационно-распорядительных документов по защите информации.

16.6. Для выявления инцидентов и реагирования на них осуществляются:

определение лиц, ответственных за выявление инцидентов и реагирование на них;

обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в автоматизированной системе управления персоналом;

анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

планирование и принятие мер по устранению инцидентов, в том числе по восстановлению автоматизированной системы управления в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

планирование и принятие мер по предотвращению повторного возникновения инцидентов.

16.7. В ходе управления конфигурацией автоматизированной системы управления и ее системы защиты осуществляются:

поддержание конфигурации автоматизированной системы управления и ее системы защиты (структуры системы защиты автоматизированной системы управления, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты (поддержание базовой конфигурации автоматизированной системы управления и ее системы защиты);

определение лиц, которым разрешены действия по внесению изменений в базовую конфигурацию автоматизированной системы управления и ее системы защиты;

регламентация и контроль технического обслуживания, в том числе дистанционного (удаленного), технических средств и программного обеспечения автоматизированной системы управления;

управление изменениями базовой конфигурации автоматизированной системы управления и ее системы защиты, в том числе определение типов возможных изменений базовой конфигурации автоматизированной системы управления и ее системы защиты, санкционирование внесения изменений в базовую конфигурацию автоматизированной системы управления и ее системы защиты, документирование действий по внесению изменений в базовую конфигурацию автоматизированной системы управления и ее системы защиты, сохранение данных об изменениях базовой конфигурации автоматизированной системы управления и ее системы защиты, контроль действий по внесению изменений в базовую конфигурацию автоматизированной системы управления и ее системы защиты;

анализ потенциального воздействия планируемых изменений в базовой конфигурации автоматизированной системы управления и ее системы защиты на обеспечение ее безопасности, возникновение дополнительных угроз безопасности информации и работоспособность автоматизированной системы управления;

определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию

автоматизированной системы управления и ее системы защиты;

внесение информации (данных) об изменениях в базовой конфигурации автоматизированной системы управления и ее системы защиты в эксплуатационную документацию на систему защиты информации автоматизированной системы управления.

16.8. В ходе контроля (мониторинга) за обеспечением уровня защищенности автоматизированной системы управления осуществляются:

контроль за событиями безопасности и действиями персонала в автоматизированной системе управления;

контроль (анализ) защищенности информации, обрабатываемой в автоматизированной системе управления, с учетом особенностей ее функционирования;

анализ и оценка функционирования системы защиты автоматизированной системы управления, включая выявление, анализ и устранение недостатков в функционировании системы защиты автоматизированной системы управления;

документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности автоматизированной системы управления;

принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности автоматизированной системы управления о необходимости пересмотра требований к защите информации в автоматизированной системе управления и доработке (модернизации) ее системы защиты.

Обеспечение защиты информации при выводе из эксплуатации автоматизированной системы управления

17. Обеспечение защиты информации при выводе из эксплуатации автоматизированной системы управления осуществляется оператором в соответствии с эксплуатационной документацией на систему защиты автоматизированной системы управления и организационно-распорядительными документами по защите информации и в том числе включает:

архивирование информации, содержащейся в автоматизированной системе управления;

уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

17.1. Архивирование информации, содержащейся в автоматизированной системе управления, должно осуществляться при необходимости дальнейшего использования информации в деятельности оператора.

17.2. Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю автоматизированной системы управления или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

При выводе автоматизированной системы управления из эксплуатации производится уничтожение машинных носителей информации, содержащих энергонезависимую память.

III. Требования к мерам защиты информации в автоматизированной системе управления

18. Организационные и технические меры защиты информации, реализуемые в автоматизированной системе управления в рамках ее системы защиты, в зависимости от класса защищенности, угроз безопасности информации, используемых технологий и структурно-функциональных характеристик автоматизированной системы управления и особенностей ее функционирования должны обеспечивать:

идентификацию и аутентификацию (ИАФ);

управление доступом (УПД);

ограничение программной среды (ОПС);

защиту машинных носителей информации (ЗНИ);
аудит безопасности (АУД);
антивирусную защиту (АВЗ);
предотвращение вторжений (компьютерных атак) (СОВ);
обеспечение целостности (ОЦЛ);
обеспечение доступности (ОДТ);
защиту технических средств и систем (ЗТС);
защиту информационной (автоматизированной) системы и ее компонентов (ЗИС);
реагирование на компьютерные инциденты (ИНЦ);
управление конфигурацией (УКФ);
управление обновлениями программного обеспечения (ОПО);
планирование мероприятий по обеспечению безопасности (ПЛН);
обеспечение действий в нештатных ситуациях (ДНС);
информирование и обучение персонала (ИПО).

Состав мер защиты информации и их базовые наборы для соответствующих классов защищенности автоматизированных систем управления приведены в приложении N 2 к настоящим Требованиям.

Содержание мер и правила их реализации устанавливаются методическим документом, разработанным ФСТЭК России в соответствии с пунктом 5 и подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085.

18.1 - 18.21. Утратили силу. - Приказ ФСТЭК России от 09.08.2018 N 138.

19. Выбор мер защиты информации для их реализации в автоматизированной системе управления в рамках ее системы защиты включает:

определение базового набора мер защиты информации для установленного класса защищенности автоматизированной системы управления в соответствии с базовыми наборами мер защиты информации, приведенными в приложении N 2 к настоящим Требованиям;

адаптацию базового набора мер защиты информации применительно к каждому уровню автоматизированной системы управления, иным структурно-функциональным характеристикам и особенностям функционирования автоматизированной системы управления (в том числе предусматривающую исключение из базового набора мер защиты информации мер, непосредственно связанных с технологиями, не используемыми в автоматизированной системе управления или ее уровнях, или структурно-функциональными характеристиками, не свойственными автоматизированной системе управления);

уточнение адаптированного базового набора мер защиты информации с учетом не выбранных ранее мер защиты информации, приведенных в приложении N 2 к настоящим Требованиям, в результате чего определяются меры защиты информации, обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации на каждом из уровней автоматизированной системы управления;

дополнение уточненного адаптированного базового набора мер защиты информации мерами, обеспечивающими выполнение требований к защите информации, установленными иными нормативными правовыми актами, локальными правовыми актами, национальными стандартами и стандартами организации в области защиты информации.

Для выбора мер защиты информации для соответствующего класса защищенности автоматизированной системы управления применяются методические документы ФСТЭК России <*>.

<*> Разработанные ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085.

20. В автоматизированной системе управления соответствующего класса защищенности в

рамках ее системы защиты должны быть реализованы меры защиты информации, выбранные в соответствии с пунктами 18 и 19 настоящих Требований и обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации на каждом из уровней автоматизированной системы управления.

Выбранные меры защиты информации рассматриваются для каждого уровня автоматизированной системы управления отдельно и подлежат реализации с учетом особенностей функционирования каждого из уровней.

При этом в автоматизированной системе управления должен быть, как минимум, реализован адаптированный для каждого уровня базовый набор мер защиты информации, соответствующий установленному классу защищенности автоматизированной системы управления.

21. В целях исключения избыточности в реализации мер защиты информации и в случае, если принятые в автоматизированной системе управления меры по обеспечению промышленной безопасности и (или) физической безопасности достаточны для блокирования (нейтрализации) отдельных угроз безопасности информации, дополнительные меры защиты информации, выбранные в соответствии с пунктами 18 и 19 настоящих Требований, могут не применяться. При этом в ходе разработки системы защиты автоматизированной системы управления должно быть проведено обоснование достаточности применения мер по обеспечению промышленной безопасности или физической безопасности для блокирования (нейтрализации) соответствующих угроз безопасности информации.

22. При отсутствии возможности реализации отдельных мер защиты информации на каком-либо из уровней автоматизированной системы управления и (или) невозможности их применения к отдельным объектам и субъектам доступа, в том числе вследствие их негативного влияния на штатный режим функционирования автоматизированной системы управления, на этапах адаптации базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации разрабатываются иные (компенсирующие) меры, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации и необходимый уровень защищенности автоматизированной системы управления.

В качестве компенсирующих мер, в первую очередь, рассматриваются меры по обеспечению промышленной и (или) физической безопасности автоматизированной системы управления, поддерживающие необходимый уровень защищенности автоматизированной системы управления.

В этом случае в ходе разработки системы защиты автоматизированной системы управления должно быть проведено обоснование применения компенсирующих мер, а при приемочных испытаниях оценена достаточность и адекватность данных компенсирующих мер для блокирования (нейтрализации) угроз безопасности информации.

23. Выбранные и реализованные в автоматизированной системе управления в рамках ее системы защиты меры защиты информации, как минимум, должны обеспечивать:

в автоматизированных системах управления 1 класса защищенности - нейтрализацию (блокирование) угроз безопасности информации, связанных с действиями нарушителя с высоким потенциалом;

в автоматизированных системах управления 2 класса защищенности - нейтрализацию (блокирование) угроз безопасности информации, связанных с действиями нарушителя с потенциалом не ниже среднего;

в автоматизированных системах управления 3 класса защищенности - нейтрализацию (блокирование) угроз безопасности информации, связанных с действиями нарушителя с низким потенциалом.

Потенциал нарушителя определяется в ходе оценки его возможностей и мотивации, проводимой при анализе угроз безопасности информации в соответствии с пунктом 13.3 настоящих Требований.

Оператором может быть принято решение о применении в автоматизированной системе управления соответствующего класса защищенности мер защиты информации,

обеспечивающих защиту от угроз безопасности информации, реализуемых нарушителем с более высоким потенциалом.

24. Технические меры защиты информации реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности. В качестве средств защиты информации в первую очередь подлежат рассмотрению механизмы защиты (параметры настройки) штатного программного обеспечения автоматизированной системы управления при их наличии.

В случае использования в автоматизированных системах управления сертифицированных по требованиям безопасности информации средств защиты информации применяются:

в автоматизированных системах управления 1 класса защищенности применяются средства защиты информации не ниже 4 класса, а также средства вычислительной техники не ниже 5 класса;

в автоматизированных системах управления 2 класса защищенности применяются средства защиты информации не ниже 5 класса, а также средства вычислительной техники не ниже 5 класса;

в автоматизированных системах управления 3 класса защищенности применяются средства защиты информации не ниже 6 класса, а также средства вычислительной техники не ниже 5 класса.

Классы защиты определяются в соответствии с нормативными правовыми актами, изданными в соответствии с подпунктом 13.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. N 1085.

В случае использования в автоматизированных системах управления средств защиты информации, сертифицированных по требованиям безопасности информации, указанные средства должны быть сертифицированы на соответствие обязательным требованиям по безопасности информации, установленным нормативными правовыми актами, или требованиям, указанным в технических условиях (заданиях по безопасности).

Функции безопасности средств защиты информации должны обеспечивать выполнение настоящих Требований.

В автоматизированных системах управления 1 и 2 классов защищенности применяются сертифицированные средства защиты информации, программное обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей.

Заказчиком (оператором) в зависимости от потенциала нарушителя может быть принято решение о повышении уровня контроля отсутствия недекларированных возможностей средств защиты информации.

25. При использовании в автоматизированных системах управления новых технологий и выявлении дополнительных угроз безопасности информации, для которых не определены меры защиты информации, должны разрабатываться компенсирующие меры в соответствии с пунктом 22 настоящих Требований.

Приложение N 1
к Требованиям 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

ОПРЕДЕЛЕНИЕ
КЛАССА ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ

1. Класс защищенности автоматизированной системы управления (первый класс (К1), второй класс (К2), третий класс (К3)) определяется в зависимости от уровня значимости (критичности) обрабатываемой в ней информации (УЗ).

2. Уровень значимости (критичности) информации (УЗ) определяется степенью возможного ущерба от нарушения ее целостности (неправомерные уничтожение или модифицирование), доступности (неправомерное блокирование) или конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), в результате которого возможно нарушение штатного режима функционирования автоматизированной системы управления или незаконное вмешательство в процессы функционирования автоматизированной системы управления.

УЗ = [(целостность, степень ущерба) (доступность, степень ущерба) (конфиденциальность, степень ущерба)],

где степень возможного ущерба определяется заказчиком или оператором экспертным или иным методом и может быть:

высокой, если в результате нарушения одного из свойств безопасности информации (целостности, доступности, конфиденциальности), повлекшего нарушение штатного режима функционирования автоматизированной системы управления, возможно возникновение чрезвычайной ситуации федерального или межрегионального характера <*> или иные существенные негативные последствия в социальной, политической, экономической, военной или иных областях деятельности;

<*> Устанавливается в соответствии с постановлением Правительства Российской Федерации от 21 мая 2007 г. N 304 "О классификации чрезвычайных ситуаций природного и техногенного характера" (Собрание законодательства Российской Федерации, 2007, N 22, ст. 2640; 2011, N 21, ст. 2971).

средней, если в результате нарушения одного из свойств безопасности информации (целостности, доступности, конфиденциальности), повлекшего нарушение штатного режима функционирования автоматизированной системы управления, возможно возникновение чрезвычайной ситуации регионального или межмуниципального характера <*> или иные умеренные негативные последствия в социальной, политической, экономической, военной или иных областях деятельности;

<*> Устанавливается в соответствии с постановлением Правительства Российской Федерации от 21 мая 2007 г. N 304 "О классификации чрезвычайных ситуаций природного и

техногенного характера" (Собрание законодательства Российской Федерации, 2007, N 22, ст. 2640; 2011, N 21, ст. 2971).

низкой, если в результате нарушения одного из свойств безопасности информации (целостности, доступности, конфиденциальности), повлекшего нарушение штатного режима функционирования автоматизированной системы управления, возможно возникновение чрезвычайной ситуации муниципального (локального) <*> характера или возможны иные незначительные негативные последствия в социальной, политической, экономической, военной или иных областях деятельности.

<*> Устанавливается в соответствии с постановлением Правительства Российской Федерации от 21 мая 2007 г. N 304 "О классификации чрезвычайных ситуаций природного и техногенного характера" (Собрание законодательства Российской Федерации, 2007, N 22, ст. 2640; 2011, N 21, ст. 2971).

В случае, если для информации, обрабатываемой в автоматизированной системе управления, не требуется обеспечение одного из свойств безопасности информации (в частности конфиденциальности) уровень значимости (критичности) определятся для двух других свойств безопасности информации (целостности, доступности). В этом случае:

УЗ = [(целостность, степень ущерба) (доступность, степень ущерба) (конфиденциальность, не применяется)].

Информация, обрабатываемая в автоматизированной системе управления, имеет высокий уровень значимости (критичности) (УЗ 1), если хотя бы для одного из свойств безопасности информации (целостности, доступности, конфиденциальности) определена высокая степень ущерба. Информация, обрабатываемая в автоматизированной системе управления, имеет средний уровень значимости (критичности) (УЗ 2), если хотя бы для одного из свойств безопасности информации (целостности, доступности, конфиденциальности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба. Информация, обрабатываемая в автоматизированной системе управления, имеет низкий уровень значимости (критичности) (УЗ 3), если для всех свойств безопасности информации (целостности, доступности, конфиденциальности) определены низкие степени ущерба.

При обработке в автоматизированной системе управления двух и более видов информации (измерительная информация, информация о состоянии процесса) уровень значимости (критичности) информации (УЗ) определяется отдельно для каждого вида информации. Итоговый уровень значимости (критичности) устанавливается по наивысшим значениям степени возможного ущерба, определенным для целостности, доступности, конфиденциальности каждого вида информации.

3. Класс защищенности автоматизированной системы управления определяется в соответствии с таблицей:Уровень значимости (критичности) информации	Класс защищенности автоматизированной системы управления
УЗ 1	К1
УЗ 2	К2
УЗ 3	К3

Приложение N 2
к Требованиям 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

СОСТАВ
МЕР ЗАЩИТЫ ИНФОРМАЦИИ И ИХ БАЗОВЫЕ НАБОРЫ
ДЛЯ СООТВЕТСТВУЮЩЕГО КЛАССА ЗАЩИЩЕННОСТИ
АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ

Условное обозначение и номер меры	Меры защиты информации в автоматизированных системах управления	Классы защищенности автоматизированной системы управления		
		3	2	1
I. Идентификация и аутентификация (ИАФ)				
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	+	+	+
II. Управление доступом (УПД)				
УПД.0	Разработка политики управления доступом	+	+	+
УПД.1	Управление учетными записями пользователей	+	+	+
УПД.2	Реализация политик управления доступа	+	+	+
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 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	+	+	+
III. Ограничение программной среды (ОПС)				
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			
IV. Защита машинных носителей информации (ЗНИ)				
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	+	+	+

V. Аудит безопасности (АУД)				
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			+
VI. Антивирусная защита (АВЗ)				
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			+
VII. Предотвращение вторжений (компьютерных атак) (СОВ)				
СОВ.0	Разработка политики предотвращения вторжений (компьютерных атак)		+	+
СОВ.1	Обнаружение и предотвращение компьютерных атак		+	+
СОВ.2	Обновление базы решающих правил		+	+
VIII. Обеспечение целостности (ОЦЛ)				
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			
IX. Обеспечение доступности (ОДТ)				
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	+	+	+
X. Защита технических средств и систем (ЗТС)				
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			
XI. Защита информационной (автоматизированной) системы и ее компонентов (ЗИС)				
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	+	+	+
XII. Реагирование на компьютерные инциденты (ИНЦ)				
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)				
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. Управление обновлениями программного обеспечения (ОПО)				
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	+	+	+
XV. Планирование мероприятий по обеспечению безопасности (ПЛН)				
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	+	+	+
XVI. Обеспечение действий в нештатных ситуациях (ДНС)				
ДНС.0	Разработка политики обеспечения действий в нештатных 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 ситуаций		+	+
ДНС.4	Резервирование программного обеспечения, технических средств, каналов связи на случай возникновения нештатных ситуаций		+	+
ДНС.5	Обеспечение возможности восстановления информационной (автоматизированной) системы в случае возникновения нештатных ситуаций	+	+	+
ДНС.6	Анализ возникших нештатных ситуаций и принятие мер по недопущению их повторного возникновения	+	+	+
XVII. Информирование и обучение персонала (ИПО)				
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	+	+	+

"+" - мера защиты информации включена в базовый набор мер для соответствующего класса защищенности автоматизированной системы управления.

Меры защиты информации, не обозначенные знаком "+", применяются при адаптации и дополнении базового набора мер, а также при разработке компенсирующих мер защиты информации в автоматизированной системе управления соответствующего класса защищенности.

ФЕДЕРАЛЬНАЯ СЛУЖБА ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

ИНФОРМАЦИОННОЕ СООБЩЕНИЕ О МЕТОДИЧЕСКИХ ДОКУМЕНТАХ ПО ВОПРОСАМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В КЛЮЧЕВЫХ СИСТЕМАХ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

от 4 мая 2018 г. N 240/22/2339

В 2005-2008 годах ФСТЭК России были разработаны и утверждены методические документы по обеспечению безопасности информации в ключевых системах информационной инфраструктуры Российской Федерации.

В связи с внесением изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. N 1085, и определением ФСТЭК России федеральным органом исполнительной власти, уполномоченным в области безопасности критической информационной инфраструктуры, с 1 января 2018 г. ФСТЭК России утратила полномочия в области обеспечения безопасности информации в ключевых системах информационной инфраструктуры.

Учитывая изложенное, в соответствии с решением директора ФСТЭК России от 3 мая 2018 г. Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, утвержденные ФСТЭК России 18 мая 2007 г., и Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, утвержденные ФСТЭК России 19 ноября 2007 г., признаны утратившими силу.

При этом Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры, утвержденная ФСТЭК России 18 мая 2007 г., а также Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры, утвержденная ФСТЭК России 18 мая 2007 г., могут применяться для моделирования угроз безопасности информации на значимых объектах критической информационной инфраструктуры Российской Федерации до утверждения ФСТЭК России соответствующих методических документов.

Заместитель директора В.Лютиков

Зарегистрировано в Минюсте России 6 сентября 2018 г. N 52109

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ
от 24 июля 2018 г. N 366

О НАЦИОНАЛЬНОМ КООРДИНАЦИОННОМ ЦЕНТРЕ ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

В соответствии с частью 4 статьи 5 и пунктом 2 части 4 статьи 6 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" <1> приказываю:

<1> Собрание законодательства Российской Федерации, 2017, N 31 (ч. I), ст. 4736.

1. Создать Национальный координационный центр по компьютерным инцидентам.

2. Утвердить прилагаемое Положение о Национальном координационном центре по компьютерным инцидентам.

Директор
А.БОРТНИКОВ

Приложение
к приказу ФСБ России
от 24 июля 2018 г. N 366

ПОЛОЖЕНИЕ
О НАЦИОНАЛЬНОМ КООРДИНАЦИОННОМ ЦЕНТРЕ
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

1. Национальный координационный центр по компьютерным инцидентам (далее - НКЦКИ) является составной частью сил, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты <1>.

<1> Пункт 2 части 2 статьи 5 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".

2. НКЦКИ в своей деятельности руководствуется законодательством Российской Федерации, ведомственными (межведомственными) нормативными правовыми актами, в том числе настоящим Положением, а также международными договорами Российской Федерации.

3. Задачей НКЦКИ является обеспечение координации деятельности субъектов критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура) по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

4. В целях выполнения предусмотренной настоящим Положением задачи НКЦКИ осуществляет следующие функции:

4.1. Координирует мероприятия по реагированию на компьютерные инциденты и непосредственно участвует в таких мероприятиях.

4.2. Организует и осуществляет обмен информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры, а также между субъектами критической информационной инфраструктуры и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, в том числе посредством использования технической инфраструктуры НКЦКИ, предназначенной для отправки, получения, обработки и хранения уведомлений и запросов в рамках информационного взаимодействия с субъектами критической информационной инфраструктуры, а также с иными не являющимися субъектами критической информационной инфраструктуры органами и организациями, в том числе иностранными и международными (далее - техническая инфраструктура НКЦКИ).

4.3. Осуществляет методическое обеспечение деятельности субъектов критической информационной инфраструктуры по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

4.4. Участвует в обнаружении, предупреждении и ликвидации последствий компьютерных атак.

4.5. Обеспечивает своевременное доведение до субъектов критической информационной инфраструктуры информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения.

4.6. Осуществляет сбор, хранение и анализ информации о компьютерных инцидентах и компьютерных атаках, а также анализ эффективности мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты.

4.7. Осуществляет эксплуатацию, обеспечение функционирования и развитие технической инфраструктуры НКЦКИ.

4.8. Организует получение информации, представляемой в соответствии с законодательством Российской Федерации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации субъектами критической информационной инфраструктуры и федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры, а также информации, которая может представляться иными не являющимися субъектами критической информационной инфраструктуры органами и организациями, в том числе иностранными и международными.

4.9. Определяет необходимые для организации взаимодействия форматы представления информации о компьютерных инцидентах в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и доводит их до субъектов критической информационной инфраструктуры.

4.10. Определяет состав технических параметров компьютерного инцидента, указываемых при представлении информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, и доводит его до субъектов критической информационной инфраструктуры.

5. В целях выполнения предусмотренных настоящим Положением задачи и функций НКЦКИ в пределах своей компетенции имеет право:

5.1. Направлять уведомления и запросы субъектам критической информационной инфраструктуры, а также иным не являющимся субъектами критической информационной инфраструктуры органам и организациям, в том числе иностранным и международным, по вопросам, связанным с обнаружением, предупреждением и ликвидацией последствий компьютерных атак и реагированием на компьютерные инциденты.

5.2. Отказывать в предоставлении информации о компьютерных инцидентах, связанных с функционированием объектов критической информационной инфраструктуры, по запросам органа иностранного государства или международной организации, не обладающих полномочиями направлять такой запрос, а также в случаях, когда предоставление такой информации создает угрозу безопасности Российской Федерации.

5.3. Создавать рабочие группы из представителей субъектов критической информационной инфраструктуры по согласованию с их руководством для решения вопросов, отнесенных к компетенции НКЦКИ.

5.4. Привлекать к реагированию на компьютерные инциденты организации и экспертов, осуществляющих деятельность в данной области.

5.5. Распространять и публиковать информационные и справочные материалы, участвовать в работе научно-технических конференций, симпозиумов, совещаний, выставок, в том числе международных, по вопросам, связанным с обнаружением, предупреждением и ликвидацией последствий компьютерных атак и реагированием на компьютерные инциденты.

5.6. Заключать от своего имени соглашения о сотрудничестве в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

6. Информационно-аналитическое, организационное и материально-техническое обеспечение НКЦКИ осуществляется Центром защиты информации и специальной связи ФСБ России.

7. НКЦКИ возглавляет директор НКЦКИ, которым является заместитель руководителя Научно-технической службы - начальник Центра защиты информации и специальной связи ФСБ России.

8. Директор НКЦКИ:

8.1. Организует деятельность НКЦКИ.

8.2. Осуществляет от имени НКЦКИ взаимодействие с субъектами критической информационной инфраструктуры, а также с иными не являющимися субъектами критической

информационной инфраструктуры органами и организациями, в том числе иностранными и международными.

8.3. Утверждает положения о рабочих группах НКЦКИ, создаваемых в соответствии с пунктом 5.3 настоящего Положения, и персональный состав таких рабочих групп.

9. НКЦКИ имеет бланк со своим наименованием и эмблему.

Зарегистрировано в Минюсте России 6 сентября 2018 г. N 52108

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ
от 24 июля 2018 г. N 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

В соответствии с пунктом 5 части 4 статьи 6 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" <1> приказываю

<1> Собрание законодательства Российской Федерации, 2017, N 31 (ч. I), ст. 4736.

утвердить:

Перечень информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (приложение N 1);

Порядок представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (приложение N 2).

Директор
А.БОРТНИКОВ

Приложение N 1
к приказу ФСБ России
от 24 июля 2018 г. N 367

ПЕРЕЧЕНЬ
ИНФОРМАЦИИ, ПРЕДСТАВЛЯЕМОЙ В ГОСУДАРСТВЕННУЮ СИСТЕМУ ОБНАРУЖЕНИЯ, ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

1. Информация, содержащаяся в реестре значимых объектов критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура).

2. Информация об отсутствии необходимости присвоения объекту критической информационной инфраструктуры одной из категорий значимости.

3. Информация об исключении объекта критической информационной инфраструктуры из реестра значимых объектов критической информационной инфраструктуры, а также об изменении категории его значимости.

4. Информация по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры о нарушении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, в результате которого создаются предпосылки возникновения компьютерных инцидентов.

5. Информация о компьютерных инцидентах, связанных с функционированием объектов критической информационной инфраструктуры:

дата, время, место нахождения или географическое местоположение объекта критической информационной инфраструктуры, на котором произошел 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.

6. Иная информация в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, предоставляемая субъектами критической информационной инфраструктуры и иными не являющимися субъектами критической информационной инфраструктуры органами и организациями, в том числе иностранными и международными.

Приложение N 2
к приказу ФСБ России
от 24 июля 2018 г. N 367

ПОРЯДОК ПРЕДСТАВЛЕНИЯ ИНФОРМАЦИИ В ГОСУДАРСТВЕННУЮ СИСТЕМУ ОБНАРУЖЕНИЯ, ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

1. Информация, указанная в пунктах 1 - 4 Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, утвержденного приказом ФСБ России от 24 июля 2018 г. N 367 (далее - Перечень), представляется в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее - ГосСОПКА) федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее - уполномоченный орган), путем ее направления в Национальный координационный центр по компьютерным инцидентам (далее - НКЦКИ) не реже раза в месяц и не позднее месячного срока с момента:

включения объекта критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура) в реестр значимых объектов критической информационной инфраструктуры;

изменения категории значимости, присвоенной значимому объекту критической информационной инфраструктуры;

получения информации об отсутствии необходимости присвоения объекту критической информационной инфраструктуры одной из категорий значимости;

исключения объекта критической информационной инфраструктуры из реестра значимых объектов критической информационной инфраструктуры;

составления акта проверки по итогам осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, в котором содержится информация о нарушении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, в результате которого создаются предпосылки возникновения компьютерных инцидентов.

2. Информация, указанная в пунктах 1 - 4 Перечня, направляется уполномоченным органом в НКЦКИ в форматах, определенных уполномоченным органом.

3. Информация, указанная в пункте 5 Перечня, представляется субъектами критической информационной инфраструктуры в ГосСОПКА путем ее направления в НКЦКИ в соответствии с определенными НКЦКИ форматами с использованием технической инфраструктуры НКЦКИ, предназначенной для отправки, получения, обработки и хранения уведомлений и запросов в рамках информационного взаимодействия с субъектами критической информационной инфраструктуры, а также с иными не являющимися субъектами критической информационной инфраструктуры органами и организациями, в том числе иностранными и международными (далее - техническая инфраструктура НКЦКИ).

4. В случае отсутствия подключения к технической инфраструктуре НКЦКИ информация направляется посредством почтовой, факсимильной или электронной связи на адреса (телефонные номера) НКЦКИ, указанные на официальном сайте в информационно-телекоммуникационной сети "Интернет" по адресу: "http://cert.gov.ru".

5. Информация, указанная в пункте 5 Перечня, направляется субъектом критической информационной инфраструктуры в НКЦКИ не позднее 24 часов с момента обнаружения компьютерного инцидента.

6. НКЦКИ уведомляет субъект критической информационной инфраструктуры о получении информации, направленной в соответствии с пунктом 5 настоящего Порядка, не позднее 24 часов с момента ее получения.

7. Информация, указанная в пункте 6 Перечня, представляется в ГосСОПКА путем ее направления в НКЦКИ посредством почтовой, факсимильной или электронной связи на адреса (телефонные номера) НКЦКИ, указанные на официальном сайте в информационно-телекоммуникационной сети "Интернет" по адресу: "http://cert.gov.ru".

8. При наличии подключения к технической инфраструктуре НКЦКИ информация, указанная в пункте 6 Перечня, направляется посредством использования данной инфраструктуры.

9. Информация, указанная в пункте 6 Перечня, представляется в ГосСОПКА в сроки, достаточные для своевременного проведения мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты.

Зарегистрировано в Минюсте России 6 сентября 2018 г. N 52107

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ
от 24 июля 2018 г. N 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

В соответствии с пунктом 7 части 4 статьи 6 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" <1> приказываю

<1> Собрание законодательства Российской Федерации, 2017, N 31 (ч. I), ст. 4736.

утвердить:

Порядок 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 (приложение N 1);

Порядок получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения (приложение N 2).

Директор
А.БОРТНИКОВ

Приложение N 1
к приказу ФСБ России
от 24 июля 2018 г. N 368

ПОРЯДОК 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

1. Настоящий Порядок определяет правила обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура), между субъектами критической информационной инфраструктуры и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты.

2. При проведении мероприятий по реагированию на компьютерные инциденты, связанные с функционированием объектов критической информационной инфраструктуры, субъекты критической информационной инфраструктуры осуществляют обмен информацией о таких компьютерных инцидентах с другими субъектами критической информационной инфраструктуры в целях минимизации последствий компьютерных инцидентов и предотвращения компьютерных инцидентов на других объектах критической информационной инфраструктуры.

Субъекты критической информационной инфраструктуры вправе самостоятельно определять круг субъектов критической информационной инфраструктуры, с которыми осуществляется такой обмен.

3. Обмен информацией о компьютерных инцидентах осуществляется в сроки, достаточные для своевременного проведения мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты.

4. Обмен информацией о компьютерных инцидентах осуществляется субъектами критической информационной инфраструктуры путем взаимного направления уведомлений в соответствии с форматами представления информации о компьютерных инцидентах в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (далее - ГосСОПКА) и составом технических параметров компьютерного инцидента, указываемых при представлении информации в ГосСОПКА, определенными Национальным координационным центром по компьютерным инцидентам (далее - НКЦКИ), а также запросов, уточняющих представляемую информацию.

5. Направление уведомлений и запросов осуществляется посредством почтовой, факсимильной, электронной или телефонной связи.

6. При наличии подключения к технической инфраструктуре НКЦКИ, предназначенной для отправки, получения, обработки и хранения уведомлений и запросов в рамках информационного взаимодействия с субъектами критической информационной инфраструктуры, а также с иными не являющимися субъектами критической информационной инфраструктуры органами и организациями, в том числе иностранными и международными

(далее - техническая инфраструктура НКЦКИ), уведомления и запросы направляются посредством использования данной инфраструктуры.

7. В случае если передаваемые в рамках обмена информацией о компьютерных инцидентах сведения составляют государственную тайну, обмен осуществляется в соответствии с требованиями законодательства Российской Федерации в области защиты государственной тайны.

8. Одновременно с направлением информации о компьютерных инцидентах в рамках обмена субъекты критической информационной инфраструктуры информируют об этом НКЦКИ.

9. Информирование в соответствии с пунктом 8 настоящего Порядка осуществляется субъектами критической информационной инфраструктуры с использованием технической инфраструктуры НКЦКИ в соответствии с форматами представления информации о компьютерных инцидентах в ГосСОПКА и составом технических параметров компьютерного инцидента, указываемых при представлении информации в ГосСОПКА, определенными НКЦКИ.

10. В случае отсутствия подключения к технической инфраструктуре НКЦКИ информирование осуществляется посредством почтовой, факсимильной или электронной связи на адреса (телефонные номера) НКЦКИ, указанные на официальном сайте в информационно-телекоммуникационной сети "Интернет" по адресу: "http://cert.gov.ru".

11. Обмен информацией о компьютерных инцидентах с уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты (далее - иностранные (международные) организации), осуществляется НКЦКИ, за исключением случаев, когда обмен субъекта критической информационной инфраструктуры такой информацией напрямую с иностранной (международной) организацией предусмотрен международным договором Российской Федерации.

12. В случае необходимости осуществления обмена информацией о компьютерном инциденте с иностранной (международной) организацией субъект критической информационной инфраструктуры направляет в НКЦКИ обращение, содержащее обоснование необходимости обмена этой информацией и указание наименования, места нахождения, адреса иностранной (международной) организации и иных необходимых для передачи информации сведений с приложением составляющей предмет обмена информации (далее - обращение).

13. Субъекты критической информационной инфраструктуры направляют обращение в НКЦКИ в порядке, установленном пунктами 9 и 10 настоящего Порядка.

14. НКЦКИ незамедлительно информирует субъект критической информационной инфраструктуры о получении его обращения.

15. НКЦКИ в течение 24 часов после получения обращения рассматривает информацию о компьютерном инциденте. В случае принятия решения о передаче этой информации в иностранную (международную) организацию, незамедлительно направляет ее адресату, о чем одновременно информируется субъект критической информационной инфраструктуры, направивший обращение.

16. При принятии НКЦКИ решения об отказе в передаче информации о компьютерном инциденте иностранной (международной) организации субъект критической информационной инфраструктуры, направивший обращение, информируется об этом в течение 24 часов.

17. Направление информации в иностранную (международную) организацию осуществляется НКЦКИ в соответствии с форматами представления информации о компьютерных инцидентах в ГосСОПКА и составом технических параметров компьютерного инцидента, указываемых при представлении информации в ГосСОПКА, определенными НКЦКИ.

18. При получении ответа от иностранной (международной) организации НКЦКИ в течение 12 часов направляет данный ответ субъекту критической информационной инфраструктуры, направившему обращение.

19. В случае если обмен информацией о компьютерных инцидентах, связанных с функционированием объектов критической информационной инфраструктуры, напрямую с иностранной (международной) организацией предусмотрен международным договором Российской Федерации, субъекты критической информационной инфраструктуры также направляют такую информацию в НКЦКИ с указанием реквизитов международного договора Российской Федерации, в соответствии с которым осуществляется данный обмен.

20. В случае получения субъектом критической информационной инфраструктуры информации о компьютерном инциденте, связанном с функционированием объекта критической информационной инфраструктуры, инициативно направленной иностранной (международной) организацией, субъект критической информационной инфраструктуры направляет полученную информацию в НКЦКИ не позднее 24 часов с момента получения такой информации.

Дальнейший обмен информацией об этом компьютерном инциденте с иностранной (международной) организацией осуществляется в соответствии с пунктами 12 - 18 настоящего Порядка.

Приложение N 2
к приказу ФСБ России
от 24 июля 2018 г. N 368

ПОРЯДОК
ПОЛУЧЕНИЯ СУБЪЕКТАМИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ ИНФОРМАЦИИ О СРЕДСТВАХ И СПОСОБАХ ПРОВЕДЕНИЯ КОМПЬЮТЕРНЫХ АТАК И О МЕТОДАХ ИХ ПРЕДУПРЕЖДЕНИЯ И ОБНАРУЖЕНИЯ

1. Настоящий Порядок определяет правила получения субъектами критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура) информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения.

2. Субъекты критической информационной инфраструктуры получают информацию о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения путем:

2.1. Обращения к официальному сайту в информационно-телекоммуникационной сети "Интернет" по адресу: "http://cert.gov.ru".

2.2. Направления запросов в Национальный координационный центр по компьютерным инцидентам (далее - НКЦКИ) с использованием технической инфраструктуры НКЦКИ, предназначенной для отправки, получения, обработки и хранения уведомлений и запросов в рамках информационного взаимодействия с субъектами критической информационной инфраструктуры, а также с иными не являющимися субъектами критической информационной инфраструктуры органами и организациями, в том числе иностранными и международными (далее - техническая инфраструктура НКЦКИ), либо, при отсутствии подключения к ней, посредством почтовой, факсимильной или электронной связи на адреса (телефонные номера) НКЦКИ, указанные на официальном сайте в информационно-телекоммуникационной сети "Интернет" по адресу: "http://cert.gov.ru".

2.3. Направления обращений в ФСБ России.

2.4. Направления запросов другим субъектам критической информационной инфраструктуры, иностранным (международным) организациям, если такой запрос не содержит сведений о компьютерных инцидентах, связанных с функционированием объектов критической информационной инфраструктуры.

3. В случае направления запроса, предусмотренного подпунктом 2.2 настоящего Порядка, ответ субъекту критической информационной инфраструктуры предоставляется в пятидневный срок с момента получения такого запроса.

4. Получение субъектами критической информационной инфраструктуры информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения в рамках обмена информацией о компьютерных инцидентах, связанных с функционированием объектов критической информационной инфраструктуры, осуществляется в соответствии с Порядком 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, утвержденным приказом ФСБ России от 24 июля 2018 г. N 368.

5. НКЦКИ осуществляет направление субъектам критической информационной инфраструктуры информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения с учетом особенностей функционирования объектов критической информационной инфраструктуры, принадлежащих данным субъектам

критической информационной инфраструктуры на праве собственности, аренды или ином законном основании.

6. Направление информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения осуществляется посредством использования технической инфраструктуры НКЦКИ.

7. В случае отсутствия у субъекта критической информационной инфраструктуры подключения к технической инфраструктуре НКЦКИ, информация направляется посредством почтовой, факсимильной или электронной связи.

8. Направление информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения субъекту критической информационной инфраструктуры осуществляется в срок не позднее 24 часов с момента получения НКЦКИ такой информации.

Зарегистрировано в Минюсте России 31 мая 2019 г. N 54801

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ
от 6 мая 2019 г. N 196

ОБ УТВЕРЖДЕНИИ ТРЕБОВАНИЙ К СРЕДСТВАМ, ПРЕДНАЗНАЧЕННЫМ ДЛЯ ОБНАРУЖЕНИЯ, ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК И РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ

В соответствии с пунктом 9 части 4 статьи 6 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" <1> приказываю

<1> Собрание законодательства Российской Федерации, 2017, N 31 (ч. I), ст. 4736.

утвердить прилагаемые Требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

Директор
А.БОРТНИКОВ

Приложение
к приказу ФСБ России
от 6 мая 2019 г. N 196

ТРЕБОВАНИЯ
К СРЕДСТВАМ, ПРЕДНАЗНАЧЕННЫМ ДЛЯ ОБНАРУЖЕНИЯ, ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК И РЕАГИРОВАНИЯ НА КОМПЬЮТЕРНЫЕ ИНЦИДЕНТЫ

I. Общие положения

1. Настоящие Требования определяют требования к устанавливаемым и используемым на всей территории Российской Федерации, в дипломатических представительствах и (или) консульских учреждениях Российской Федерации техническим, программным, программно-аппаратным и иным средствам для обнаружения (в том числе для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура), предупреждения, ликвидации последствий компьютерных атак и (или) обмена информацией, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак, а также криптографическим средствам защиты такой информации (далее - средства ГосСОПКА).

2. К средствам ГосСОПКА относятся:

технические, программные, программно-аппаратные и иные средства для обнаружения компьютерных атак (далее - средства обнаружения);

технические, программные, программно-аппаратные и иные средства для предупреждения компьютерных атак (далее - средства предупреждения);

технические, программные, программно-аппаратные и иные средства для ликвидации последствий компьютерных атак (далее - средства ликвидации последствий);

технические, программные, программно-аппаратные и иные средства поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры (далее - средства ППКА);

технические, программные, программно-аппаратные и иные средства обмена информацией, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак (далее - средства обмена);

криптографические средства защиты информации, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак.

Средства ГосСОПКА реализуются одним или несколькими техническими, программными и программно-аппаратными средствами.

II. Требования к средствам ГосСОПКА

3. Средства ГосСОПКА должны соответствовать следующим требованиям:

3.1. В средствах ГосСОПКА должна быть исключена возможность удаленного управления со стороны лиц, не являющихся работниками субъекта критической информационной инфраструктуры и (или) работниками привлекаемой в соответствии с законодательством Российской Федерации субъектом критической информационной инфраструктуры организации, осуществляющей лицензируемую деятельность в области

защиты информации.

3.2. В средствах ГосСОПКА должна быть исключена возможность несанкционированной передачи обрабатываемой информации лицам, не являющимся работниками субъекта критической информационной инфраструктуры и (или) работниками привлекаемой в соответствии с законодательством Российской Федерации субъектом критической информационной инфраструктуры организации, осуществляющей лицензируемую деятельность в области защиты информации.

3.3. Средства ГосСОПКА должны иметь возможность модернизации российскими организациями, не находящимися под прямым или косвенным контролем иностранных физических лиц и (или) юридических лиц.

3.4. Средства ГосСОПКА должны быть обеспечены гарантийной и технической поддержкой российскими организациями, не находящимися под прямым или косвенным контролем иностранных физических лиц и (или) юридических лиц.

3.5. Работа средств ГосСОПКА не должна приводить к нарушениям функционирования информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления, находящихся на территории Российской Федерации, в дипломатических представительствах и (или) консульских учреждениях Российской Федерации (далее - информационные ресурсы) (должно быть исключено влияние на достижение целей и функционирование объектов критической информационной инфраструктуры).

3.6. В средствах ГосСОПКА должны быть реализованы функции безопасности в соответствии с главой VIII настоящих Требований.

III. Требования к средствам обнаружения

4. Средства обнаружения должны обладать следующими функциями:

сбор и первичная обработка событий, связанных с нарушением информационной безопасности (далее - события ИБ), поступающих от операционных систем, средств обнаружения вторжений, межсетевых экранов, средств предотвращения утечек данных, антивирусного программного обеспечения, телекоммуникационного оборудования, прикладных сервисов, средств контроля (анализа) защищенности, средств управления телекоммуникационным оборудованием и сетями связи, систем мониторинга состояния телекоммуникационного оборудования, систем мониторинга качества обслуживания, а также иных средств и систем защиты информации и систем мониторинга, эксплуатируемых субъектом критической информационной инфраструктуры (далее - источники событий ИБ);

автоматический анализ событий ИБ и выявление компьютерных инцидентов;

повторный анализ ранее зарегистрированных событий ИБ и выявление на основе такого анализа не обнаруженных ранее компьютерных инцидентов.

5. При осуществлении сбора и первичной обработки событий ИБ средства обнаружения должны обеспечивать:

удаленный и (или) локальный сбор событий ИБ;

сбор событий ИБ в непрерывном режиме функционирования либо по расписанию, в случае потери связи с источниками событий ИБ - сразу после ее восстановления;

обработку поступающих событий ИБ и сохранение результатов их обработки;

сохранение информации о событиях ИБ, в том числе в исходном виде;

сбор информации непосредственно от источников событий ИБ, из файлов либо посредством агентов, размещенных на отдельных источниках событий ИБ;

встроенную поддержку различных источников событий ИБ и возможность разработки дополнительных модулей, обеспечивающих получение информации от новых источников событий ИБ.

6. При осуществлении автоматического анализа событий ИБ и выявления

компьютерных инцидентов средства обнаружения должны обеспечивать:

отбор и фильтрацию событий ИБ;

выявление последовательностей разнородных событий ИБ, имеющих логическую связь, которые могут быть значимы для выявления возможных нарушений безопасности информации (корреляция) и объединение однородных данных о событиях ИБ (агрегация);

выявление компьютерных инцидентов, регистрацию методов (способов) их обнаружения;

возможность корреляции для распределенных по времени и (или) месту возникновения событий ИБ;

возможность корреляции для последовательности событий ИБ;

возможность просмотра и редактирования правил корреляции, а также обновления и загрузки новых правил;

автоматическое назначение приоритетов событиям ИБ на основании задаваемых пользователем показателей.

7. При осуществлении повторного анализа ранее зарегистрированных событий ИБ и выявления на основе такого анализа не обнаруженных ранее компьютерных инцидентов средства обнаружения должны обеспечивать:

выявление связей и зависимостей между событиями ИБ, зарегистрированными в установленном интервале времени, и вновь появившейся любой дополнительной информацией, позволяющей идентифицировать контролируемые информационные ресурсы (далее - справочная информация);

выявление связей и зависимостей между событиями ИБ, зарегистрированными в установленном интервале времени, и новыми или измененными методами (способами) выявления компьютерных инцидентов;

выявление связей и зависимостей между событиями ИБ и полученными ранее сведениями о контролируемых информационных ресурсах и (или) о состоянии защищенности;

возможность настройки параметров проводимого анализа;

проведение поиска не обнаруженных ранее компьютерных инцидентов с использованием новых методов (способов) выявления компьютерных инцидентов;

хранение агрегированных событий ИБ не менее шести месяцев.

IV. Требования к средствам предупреждения

8. Средства предупреждения должны обладать следующими функциями:

сбор и обработка сведений об инфраструктуре контролируемых информационных ресурсов и справочной информации;

сбор и обработка сведений об уязвимостях и недостатках в настройке программного обеспечения (далее - ПО), используемого в контролируемых информационных ресурсах;

формирование рекомендаций по минимизации угроз безопасности информации;

учет угроз безопасности информации.

9. При осуществлении сбора и обработки сведений об инфраструктуре контролируемых информационных ресурсов и справочной информации средства предупреждения должны обеспечивать:

9.1. Сбор и обработку сведений об инфраструктуре контролируемых информационных ресурсов, включающих информацию:

об архитектуре и объектах контролируемых информационных ресурсов (сетевые адреса и имена, наименования и версии используемого ПО);

о выполняющихся на объектах контролируемых информационных ресурсов сетевых службах;

об источниках событий ИБ.

9.2. Сбор и обработку справочной информации:

о показателе доверия (репутации) сетевых адресов, доменных имен, серверов электронной почты, серверов доменных имен;

о владельцах сетевых адресов, доменных имен, серверов электронной почты, серверов доменных имен;

о местоположении и географической принадлежности сетевых адресов;

об известных уязвимостях используемого ПО;

о компьютерных сетях, состоящих из управляемых с использованием вредоносного ПО средств вычислительной техники, включая сведения об их управляющих серверах.

9.3. Возможность добавления, просмотра и изменения сведений об инфраструктуре контролируемых информационных ресурсов и справочной информации.

10. При осуществлении сбора и обработки сведений об уязвимостях и недостатках в настройке ПО, используемого в контролируемых информационных ресурсах, средства предупреждения должны обеспечивать:

сбор данных о дате и времени проведения исследования контролируемых информационных ресурсов;

формирование перечня выявленных уязвимостей и недостатков в настройке используемого ПО (для каждого объекта контролируемого информационного ресурса);

возможность статистической и аналитической обработки полученной информации.

11. Формируемые рекомендации по минимизации угроз безопасности информации должны содержать перечень мер, направленных на устранение уязвимостей и недостатков в настройке ПО, используемого в контролируемых информационных ресурсах.

12. При осуществлении учета угроз безопасности информации средства предупреждения должны обеспечивать:

создание и изменение записи, содержащей уведомление об угрозе безопасности информации в форматах, обрабатываемых технической инфраструктурой Национального координационного центра по компьютерным инцидентам <1> (далее - НКЦКИ), предназначенной для отправки, получения, обработки и хранения уведомлений и запросов в рамках информационного взаимодействия с субъектами критической информационной инфраструктуры, а также с иными не являющимися субъектами критической информационной инфраструктуры органами и организациями, в том числе иностранными и международными;

<1> Подпункт 4.9 пункта 4 Положения о Национальном координационном центре по компьютерным инцидентам, утвержденного приказом ФСБ России от 24 июля 2018 г. N 366 "О Национальном координационном центре по компьютерным инцидентам" (зарегистрирован Минюстом России 6 сентября 2018 г., регистрационный N 52109).

создание и изменение инструкций по реагированию на компьютерные инциденты, связанные с угрозами безопасности информации, включающих порядок принятия решений, очередность выполняемых действий и способы организации совместных действий участвующих в мероприятиях по реагированию на компьютерные инциденты и ликвидации последствий компьютерных атак работников субъекта критической информационной инфраструктуры и (или) работников привлекаемой в соответствии с законодательством Российской Федерации субъектом критической информационной инфраструктуры организации, осуществляющей лицензируемую деятельность в области защиты информации;

создание и изменение инструкций по обработке запросов и уведомлений, поступающих из НКЦКИ.

V. Требования к средствам ликвидации последствий

13. Средства ликвидации последствий должны обладать следующими функциями:

учет и обработка компьютерных инцидентов;

управление процессами реагирования на компьютерные инциденты и ликвидации последствий компьютерных атак;

взаимодействие с НКЦКИ посредством использования технической инфраструктуры НКЦКИ, предназначенной для отправки, получения, обработки и хранения уведомлений и запросов в рамках информационного взаимодействия с субъектами критической информационной инфраструктуры, а также с иными не являющимися субъектами критической информационной инфраструктуры органами и организациями, в том числе иностранными и международными;

информационно-аналитическое сопровождение пользователей.

14. При осуществлении учета и обработки компьютерных инцидентов средства ликвидации последствий должны обеспечивать:

создание и изменение формализованных описаний (далее - карточка) компьютерных инцидентов, определение типов компьютерных инцидентов, определение состава полей карточек и требований к их заполнению в соответствии с типом компьютерного инцидента;

автоматическое создание карточки компьютерного инцидента на основе уведомления об угрозе безопасности информации либо при выявлении события ИБ, в котором содержатся признаки компьютерных атак для контролируемых информационных ресурсов;

запись о текущей стадии процесса реагирования на компьютерные инциденты (стадия приема сообщения о компьютерном инциденте, стадия сбора первичных сведений о компьютерном инциденте, стадия локализации компьютерного инцидента, стадия сбора сведений для расследования компьютерного инцидента) в зависимости от типа компьютерного инцидента;

запись о присвоении категорий опасности и (или) определение приоритетов компьютерных инцидентов на основе критериев, задаваемых по значениям полей карточек компьютерных инцидентов;

регистрацию и учет карточек компьютерных инцидентов;

фильтрацию, сортировку и поиск карточек компьютерных инцидентов по значениям полей карточек;

объединение карточек компьютерных инцидентов на основе критериев, применяемых к значениям полей карточек.

15. Для обеспечения управления процессами реагирования на компьютерные инциденты и ликвидации последствий компьютерных атак средства ликвидации последствий должны обеспечивать:

возможность включения в карточку компьютерного инцидента дополнительных сведений, связанных с компьютерным инцидентом и зарегистрированных в процессе реагирования на компьютерный инцидент и ликвидации последствий компьютерной атаки, в том числе сообщений пользователей контролируемых информационных ресурсов, сведений о предпринятых действиях, технических данных, необходимых для расследования обстоятельств компьютерного инцидента;

возможность назначения для карточки компьютерного инцидента инструкций по реагированию на компьютерный инцидент, а также задания правил их применимости на основании сведений о компьютерном инциденте;

формирование электронных сообщений для организации взаимодействия и координации действий работников субъекта критической информационной инфраструктуры и (или) работников привлекаемой в соответствии с законодательством Российской Федерации субъектом критической информационной инфраструктуры организации, осуществляющей лицензируемую деятельность в области защиты информации, участвующих в реагировании на компьютерный инцидент и ликвидации последствий компьютерной атаки.

16. При взаимодействии с НКЦКИ средства ликвидации последствий должны обеспечивать:

автоматизированный обмен информацией, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, указанной в пункте 5 Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, утвержденного приказом ФСБ России от 24 июля 2018 г. N 367 <1>;

учет карточек компьютерных инцидентов в соответствии с идентификацией НКЦКИ.

<1> Зарегистрирован Минюстом России 6 сентября 2018 г., регистрационный N 52108.

17. При осуществлении информационно-аналитического сопровождения средства ликвидации последствий должны обеспечивать формирование выборок данных, основанных на значениях полей карточек компьютерных инцидентов, уведомлений об актуальных угрозах безопасности информации и справочной информации.

VI. Требования к средствам ППКА

18. Средства ППКА должны обладать следующими функциями:

обнаружение признаков компьютерных атак в сети электросвязи по значениям служебных полей протоколов сетевого взаимодействия, а также осуществление сбора, накопления и статистической обработки результатов такого обнаружения;

обнаружение в сети электросвязи признаков управления телекоммуникационным оборудованием;

обнаружение изменений параметров настроек телекоммуникационного оборудования сети электросвязи;

обнаружение изменений параметров настроек систем управления телекоммуникационным оборудованием и сетями электросвязи;

хранение копий сетевого трафика, в котором были обнаружены признаки компьютерных атак в сети электросвязи и (или) признаки управления телекоммуникационным оборудованием, не менее шести месяцев;

анализ и экспорт фрагментов копий сетевого трафика, в котором были обнаружены признаки компьютерных атак в сети электросвязи и (или) признаки управления телекоммуникационным оборудованием;

уведомление о фактах обнаружения признаков компьютерных атак в сети электросвязи и (или) признаков управления телекоммуникационным оборудованием;

уведомление о фактах нарушения режимов функционирования средств ППКА;

наличие интерфейса(ов) передачи фрагментов копий сетевого трафика, в котором обнаружены признаки компьютерных атак в сети электросвязи и (или) признаки управления телекоммуникационным оборудованием, а также результатов сбора, накопления и статистической обработки такой информации;

возможность формирования информации, предусмотренной пунктом 5 Перечня, указанного в пункте 16 настоящих Требований.

VII. Требования к средствам обмена и криптографическим средствам защиты информации, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак

19. Средства обмена должны обеспечивать передачу, прием и целостность при передаче и приеме информации, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий

компьютерных атак.

20. Криптографические средства защиты информации, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак, должны быть сертифицированы в системе сертификации средств криптографической защиты информации.

VIII. Требования к средствам ГосСОПКА в части реализации функций безопасности

21. Средства ГосСОПКА в части реализации функций безопасности должны обеспечивать:

идентификацию и аутентификацию пользователей;

разграничение прав доступа к информации и функциям;

регистрацию событий ИБ;

обновление программных компонентов и служебных баз данных;

резервирование и восстановление своей работоспособности;

синхронизацию системного времени и корректировку временных значений (корректировку настроек часовых поясов);

контроль целостности ПО.

21.1. При осуществлении идентификации и аутентификации пользователей средства ГосСОПКА должны обеспечивать:

аутентификацию пользователей с использованием паролей (в том числе временного действия) и (или) аппаратных средств аутентификации;

хранение паролей в зашифрованном виде;

автоматическое информирование о необходимости смены паролей.

21.2. При осуществлении разграничения прав доступа к информации и функциям средства ГосСОПКА должны обеспечивать:

поддержку функций создания, редактирования и удаления пользовательских ролей и возможность настройки прав доступа для каждой роли;

возможность блокирования и повторной активации учетных записей;

блокирование сессии доступа при превышении задаваемого значения временного периода отсутствия активности;

уведомление о неудачных попытках доступа к управлению средствами ГосСОПКА;

запись всех действий пользователей с момента авторизации в электронный журнал.

21.3. При осуществлении регистрации событий ИБ средства ГосСОПКА должны обеспечивать:

возможность определения перечня событий ИБ, подлежащих регистрации, и хранения соответствующих записей в электронных журналах с возможностью корректировки сроков;

возможность регистрации следующих связанных с функционированием средств ГосСОПКА сведений: идентификатора пользователя, времени авторизации, запуска (завершения) программ и процессов, связанных с реализацией функций безопасности средств ГосСОПКА, команды управления, неудачных попыток аутентификации, данных о сбоях и неисправностях в работе средств ГосСОПКА;

ведение электронных журналов учета технического состояния, содержащих следующие поля: информация о состоянии интерфейсов (портов), информация об ошибках в работе средств ГосСОПКА с их классификацией, информация о загрузке и инициализации средств ГосСОПКА и их остановке (только для средств ППКА);

защиту электронных журналов от редактирования и удаления содержащейся в них информации (только для средств ППКА);

автоматическое уведомление о заполнении электронного журнала и возможность его сохранения на внешнем носителе информации (только для средств ППКА).

21.4. При осуществлении обновления программных компонентов и служебных баз

данных средства ГосСОПКА должны обеспечивать:

обновление без потери информации, необходимой для функционирования средств, а также информации о компьютерных инцидентах и событиях ИБ;

обновление только пользователями, ответственными за управление (администрирование) средств ГосСОПКА;

восстановление работоспособности в случае сбоя процесса обновления (в том числе осуществление предварительного резервного копирования и последующее восстановление).

21.5. При осуществлении резервирования и восстановления своей работоспособности средства ГосСОПКА должны обеспечивать:

возможность создания резервной копии конфигурационных данных на внешнем носителе;

возможность создания резервной копии ПО на внешнем носителе;

возможность самовосстановления работоспособности при обнаружении критических ошибок в процессе функционирования (только для средств ППКА).

21.6. При осуществлении контроля целостности ПО средства ГосСОПКА должны обеспечивать:

проверку целостности ПО и конфигурационных файлов при загрузке, во время функционирования и по команде пользователя, ответственного за управление (администрирование) средством ГосСОПКА;

возможность штатного самотестирования ПО в процессе функционирования;

регистрацию в электронном журнале результатов проведения контроля целостности ПО.

IX. Требования к средствам обнаружения, средствам предупреждения и средствам ликвидации последствий в части реализации визуализации, построения сводных отчетов и хранения информации

22. К средствам обнаружения, средствам предупреждения и средствам ликвидации последствий предъявляются требования в части реализации визуализации, построения сводных отчетов и хранения информации.

Средства обнаружения, средства предупреждения и средства ликвидации последствий должны обеспечивать:

22.1. Визуализацию в виде таблиц (списков, схем, графиков, диаграмм) сведений:

о событиях ИБ;

об обнаруженных компьютерных инцидентах;

об уязвимостях и недостатках в настройке ПО, используемого в контролируемых информационных ресурсах;

об инфраструктуре контролируемых информационных ресурсов;

хранящихся в базе данных;

содержащих справочную и другую необходимую информацию.

22.2. Построение сводных отчетов путем реализации следующих функций:

создание таблиц (списков, схем, графиков, диаграмм), а также их визуализация на основе полученных данных;

выбор параметров, по которым строятся таблицы (списки, схемы, графики, диаграммы) в отчетах;

экспорт отчетов;

автоматическое формирование отчетов по расписанию, а также их автоматическое направление назначаемым адресатам.

22.3. Хранение загружаемой информации в течение установленного периода времени и постоянный доступ к ней, а также возможность экспорта хранящейся информации, в том

числе в исходном виде.

Зарегистрировано в Минюсте России 16 июля 2019 г. N 55285

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ
от 19 июня 2019 г. N 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 КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

В соответствии с пунктом 10 части 4 статьи 6 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" <1> приказываю

<1> Собрание законодательства Российской Федерации, 2017, N 31 (ч. I), ст. 4736.

утвердить прилагаемые Порядок, технические условия 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 критической информационной инфраструктуры Российской Федерации.

Директор
А.БОРТНИКОВ

Приложение
к приказу ФСБ России
от 19 июня 2019 г. N 281

ПОРЯДОК, ТЕХНИЧЕСКИЕ УСЛОВИЯ 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 КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

1. Настоящие Порядок и технические условия регулируют установку и эксплуатацию 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 критической информационной инфраструктуры Российской Федерации (далее - средства, критическая информационная инфраструктура соответственно), в том числе в банковской сфере и в иных сферах финансового рынка.

2. Для согласования установки средств субъект критической информационной инфраструктуры не позднее чем за 45 календарных дней до даты планируемой установки направляет в ФСБ России структурно-функциональную схему подключения средств к информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, а также сведения:

об устанавливаемых средствах (наименование, предназначение, версия (при наличии);

о местах установки средств (место нахождения или географическое местоположение зданий или сооружений, в которых планируется установка средств);

о лицах, ответственных за эксплуатацию средств (фамилия, имя, отчество (при наличии), должность, телефонные номера);

о контролируемых средствами объектах критической информационной инфраструктуры (наименования информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления).

3. ФСБ России в срок до 45 календарных дней с даты поступления рассматривает представленные сведения на предмет отсутствия или наличия оснований для отказа в согласовании установки средств.

По результатам рассмотрения представленных сведений ФСБ России подготавливает и направляет субъекту критической информационной инфраструктуры письмо о согласовании или об отказе в согласовании установки средств.

4. Субъект критической информационной инфраструктуры, который осуществляет деятельность в банковской сфере и в иных сферах финансового рынка, должен направить информацию, указанную в пункте 2 настоящих Порядка и технических условий, в Банк России в течение 5 календарных дней с даты получения письма ФСБ России о согласовании.

5. Изменение структурно-функциональной схемы подключения средств к информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, состава установленных средств и (или) мест их установки осуществляется субъектом критической информационной инфраструктуры по согласованию с ФСБ России в порядке, предусмотренном пунктом 2 настоящих Порядка и технических условий.

При изменении иной информации, указанной в пункте 2 настоящих Порядка и технических условий, субъект критической информационной инфраструктуры информирует ФСБ России в течение 5 календарных дней со дня ее изменения.

При изменении информации, указанной в пункте 2 настоящих Порядка и технических условий, субъект критической информационной инфраструктуры, который осуществляет деятельность в банковской сфере и в иных сферах финансового рынка, информирует Банк России в течение 5 календарных дней со дня ее изменения.

6. Установка, настройка, проверка работоспособности и подключение средств к информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления проводятся субъектом критической информационной инфраструктуры и (или) привлекаемой в соответствии с законодательством Российской Федерации субъектом критической информационной инфраструктуры организацией, осуществляющей лицензируемую деятельность в области защиты информации, и осуществляются в соответствии с эксплуатационной документацией на данные средства. При этом установка средств не должна нарушать функционирование информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления объекта критической информационной инфраструктуры.

7. Субъект критической информационной инфраструктуры после приема в эксплуатацию средств информирует об этом Национальный координационный центр по компьютерным инцидентам <1> в течение 5 календарных дней.

<1> Положение о Национальном координационном центре по компьютерным инцидентам, утвержденное приказом ФСБ России от 24 июля 2018 г. N 366 "О Национальном координационном центре по компьютерным инцидентам" (зарегистрирован Минюстом России 6 сентября 2018 г., регистрационный N 52109).

8. В целях непрерывного взаимодействия с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации субъект критической информационной инфраструктуры обеспечивает круглосуточную и бесперебойную работу средств.

9. Субъект критической информационной инфраструктуры определяет порядок доступа к эксплуатируемым средствам и осуществления контроля за ним.

10. Эксплуатация и техническое обслуживание средств осуществляется субъектом критической информационной инфраструктуры и (или) привлекаемой в соответствии с законодательством Российской Федерации субъектом критической информационной инфраструктуры организацией, осуществляющей лицензируемую деятельность в области защиты информации, в соответствии с эксплуатационной документацией на данные средства.

11. При аварийном отключении электропитания субъект критической информационной инфраструктуры должен обеспечивать работу средств в текущем режиме или правильное (корректное) завершение их работы с реализацией функции автоматического оповещения лиц, ответственных за эксплуатацию средств.

Зарегистрировано в Минюсте России 16 июля 2019 г. N 55284

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ
от 19 июня 2019 г. N 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 КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Список изменяющих документов
(в ред. Приказа ФСБ России от 07.07.2022 N 348)

В соответствии с пунктом 6 части 4 статьи 6 Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации" <1> приказываю

<1> Собрание законодательства Российской Федерации, 2017, N 31 (ч. I), ст. 4736.

утвердить прилагаемый Порядок информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации.

Директор
А.БОРТНИКОВ

Приложение
к приказу ФСБ России
от 19 июня 2019 г. N 282

ПОРЯДОК ИНФОРМИРОВАНИЯ ФСБ РОССИИ О КОМПЬЮТЕРНЫХ ИНЦИДЕНТАХ, РЕАГИРОВАНИЯ НА НИХ, ПРИНЯТИЯ МЕР ПО ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК, ПРОВЕДЕННЫХ В ОТНОШЕНИИ ЗНАЧИМЫХ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Список изменяющих документов
(в ред. Приказа ФСБ России от 07.07.2022 N 348)

1. Настоящий Порядок определяет процедуру информирования ФСБ России субъектами критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура) о компьютерных инцидентах, а также реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры, в том числе в банковской сфере и в иных сферах финансового рынка.

2. Субъекты критической информационной инфраструктуры информируют ФСБ России обо всех компьютерных инцидентах, связанных с функционированием принадлежащих им на праве собственности, аренды или ином законном основании объектов критической информационной инфраструктуры.

3. Информирование осуществляется путем направления информации в Национальный координационный центр по компьютерным инцидентам <1> (далее - НКЦКИ) в соответствии с определенными НКЦКИ форматами <2> представления информации о компьютерных инцидентах в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации с использованием технической инфраструктуры НКЦКИ, предназначенной для отправки, получения, обработки и хранения уведомлений и запросов в рамках информационного взаимодействия с субъектами критической информационной инфраструктуры, а также с иными, не являющимися субъектами критической информационной инфраструктуры, органами и организациями, в том числе иностранными и международными.

<1> Положение о Национальном координационном центре по компьютерным инцидентам, утвержденное приказом ФСБ России от 24 июля 2018 г. N 366 (зарегистрирован Минюстом России 6 сентября 2018 г., регистрационный N 52109) (далее - Положение о НКЦКИ).
(сноска в ред. Приказа ФСБ России от 07.07.2022 N 348)

<2> Подпункт 4.9 пункта 4 Положения о НКЦКИ.
(сноска в ред. Приказа ФСБ России от 07.07.2022 N 348)

В случае отсутствия подключения к данной технической инфраструктуре информация

передается субъектом критической информационной инфраструктуры посредством почтовой, факсимильной или электронной связи на адреса (телефонные номера) НКЦКИ, указанные на официальном сайте в информационно-телекоммуникационной сети "Интернет" по адресу: "http://cert.gov.ru".

4. Информация о компьютерном инциденте, связанном с функционированием значимого объекта критической информационной инфраструктуры, направляется субъектом критической информационной инфраструктуры в НКЦКИ в срок не позднее 3 часов с момента обнаружения компьютерного инцидента, а в отношении иных объектов критической информационной инфраструктуры - в срок не позднее 24 часов с момента его обнаружения.

5. В случае если компьютерный инцидент связан с функционированием объекта критической информационной инфраструктуры, принадлежащего на праве собственности, аренды или ином законном основании субъекту критической информационной инфраструктуры, который осуществляет деятельность в банковской сфере и в иных сферах финансового рынка, информация о компьютерном инциденте также направляется в Банк России с использованием технической инфраструктуры Банка России в сроки, установленные пунктом 4 настоящего Порядка.

В случае отсутствия возможности уведомления субъектом критической информационной инфраструктуры, который осуществляет деятельность в банковской сфере и в иных сферах финансового рынка, посредством технической инфраструктуры Банка России информация передается субъектом критической информационной инфраструктуры в Банк России посредством почтовой, факсимильной или электронной связи на адреса (телефонные номера), указанные на официальном сайте Банка России в информационно-телекоммуникационной сети "Интернет".

6. Для подготовки к реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак субъектом критической информационной инфраструктуры, которому на праве собственности, аренды или ином законном основании принадлежит значимый объект критической информационной инфраструктуры, в срок до 90 календарных дней со дня включения данного объекта в реестр значимых объектов критической информационной инфраструктуры Российской Федерации <1> разрабатывается план реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак (далее - План), содержащий:

<1> Порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденный приказом ФСТЭК России от 6 декабря 2017 г. N 227 (зарегистрирован Минюстом России 8 февраля 2018 г., регистрационный N 49966), с изменениями, внесенными приказом ФСТЭК России от 10 февраля 2022 г. N 26 (зарегистрирован Минюстом России 1 апреля 2022 г., регистрационный N 68031).
(сноска в ред. Приказа ФСБ России от 07.07.2022 N 348)

технические характеристики и состав значимых объектов критической информационной инфраструктуры;

события (условия), при наступлении которых начинается реализация предусмотренных Планом мероприятий;

мероприятия, проводимые в ходе реагирования на компьютерные инциденты и

принятия мер по ликвидации последствий компьютерных атак, а также время, отводимое на их реализацию;

описание состава подразделений и должностных лиц субъекта критической информационной инфраструктуры, ответственных за проведение мероприятий по реагированию на компьютерные инциденты и принятие мер по ликвидации последствий компьютерных атак.

Разработанный План утверждается руководителем субъекта критической информационной инфраструктуры (индивидуальным предпринимателем - субъектом критической информационной инфраструктуры), которому на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры. Копия утвержденного Плана в срок до 7 календарных дней со дня утверждения направляется в НКЦКИ.
(абзац введен Приказом ФСБ России от 07.07.2022 N 348)

7. При необходимости в План включаются:

условия привлечения подразделений и должностных лиц ФСБ России к проведению мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак;

порядок проведения субъектом критической информационной инфраструктуры, которому на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак в отношении значимых объектов критической информационной инфраструктуры совместно с привлекаемыми подразделениями и должностными лицами ФСБ России.

8. Проект Плана, содержащий положения, предусмотренные пунктом 7 настоящего Порядка, разрабатывается субъектом критической информационной инфраструктуры при методическом обеспечении НКЦКИ <1> и до его утверждения направляется на согласование в ФСБ России.
(в ред. Приказа ФСБ России от 07.07.2022 N 348)

<1> Подпункт 4.3 пункта 4 Положения о НКЦКИ.
(сноска введена Приказом ФСБ России от 07.07.2022 N 348)

ФСБ России рассматривает проект Плана в срок до 30 календарных дней и по результатам рассмотрения согласовывает его или возвращает без согласования для доработки.

9. План, разрабатываемый субъектами критической информационной инфраструктуры, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, осуществляющими деятельность в банковской сфере и в иных сферах финансового рынка, должен включать, помимо положений, указанных в пунктах 6 и 7 настоящего Порядка, условия привлечения подразделений и должностных лиц Банка России к проведению мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак. Такой План и изменения в него согласовываются с Банком России.

10. Субъект критической информационной инфраструктуры, которому на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, не реже одного раза в год организует и проводит тренировки по отработке мероприятий Плана. Объем и содержание тренировки определяются субъектом критической информационной инфраструктуры с учетом мероприятий, содержащихся в Плане.

Организация и проведение тренировок возлагаются на подразделения и должностных лиц субъекта критической информационной инфраструктуры, ответственных за проведение мероприятий по реагированию на компьютерные инциденты и принятие мер по ликвидации последствий компьютерных атак.

При необходимости по результатам тренировок в План вносятся изменения.

11. Субъект критической информационной инфраструктуры, которому на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, в ходе реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак осуществляет:

анализ компьютерных инцидентов (включая определение очередности реагирования на них), установление их связи с компьютерными атаками;

проведение мероприятий в соответствии с Планом;

определение в соответствии с Планом необходимости привлечения к реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак подразделений и должностных лиц ФСБ России и Банка России.

12. Перед принятием мер по ликвидации последствий компьютерных атак субъект критической информационной инфраструктуры, которому на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, определяет:

состав подразделений и должностных лиц субъекта критической информационной инфраструктуры, ответственных за проведение мероприятий по реагированию на компьютерные инциденты и принятие мер по ликвидации последствий компьютерных атак, и их задачи в рамках принимаемых мер;

перечень средств, необходимых для принятия мер по ликвидации последствий компьютерных атак;

очередность значимых объектов критической информационной инфраструктуры (их структурных элементов), в отношении которых будут приниматься меры по ликвидации последствий компьютерных атак;

перечень мер по восстановлению функционирования значимого объекта критической информационной инфраструктуры.

13. В ходе ликвидации последствий компьютерных атак субъектом критической информационной инфраструктуры, которому на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, принимаются меры по восстановлению функционирования и проверке работоспособности значимого объекта критической информационной инфраструктуры.

14. О результатах мероприятий по реагированию на компьютерные инциденты и

принятию мер по ликвидации последствий компьютерных атак субъект критической информационной инфраструктуры, которому на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, информирует НКЦКИ в срок не позднее 48 часов после завершения таких мероприятий в соответствии с пунктом 3 настоящего Порядка.

Субъекты критической информационной инфраструктуры, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, осуществляющие деятельность в банковской сфере и в иных сферах финансового рынка, наряду с НКЦКИ информируют о результатах мероприятий по реагированию на компьютерные инциденты и принятию мер по ликвидации последствий компьютерных атак Банк России в срок не позднее 48 часов после завершения таких мероприятий в соответствии с пунктом 5 настоящего Порядка.