КОМИТЕТ
ЦИФРОВОГО РАЗВИТИЯ
ЛЕНИНГРАДСКОЙ ОБЛАСТИ

ПРИКАЗ

от 6 октября 2020 года № 19

Об утверждении Правил выявления инцидентов, которые могут привести к сбоям или нарушению функционирования государственных информационных систем Ленинградской области и объектов критической информационной инфраструктуры Ленинградской области и (или) к возникновению угроз безопасности информации, и реагирования на них

В соответствии п. 2.11, 2.12, 2.13 Положения о Комитете цифрового развития Ленинградской области, утвержденного постановлением Правительства Ленинградской области 05.08.2019 № 364, п. 4 Порядка взаимодействия органов исполнительной власти Ленинградской области при создании, модернизации и развитии государственных информационных систем Ленинградской области, утвержденного постановлением Правительства Ленинградской области от 20 июня 2019 года № 287, п. 16.2, 18.1, 18.3 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 N 17, п. ИНЦ.0 Приложения к Требованиям по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденным приказом ФСТЭК России от 25 декабря 2017 г. № 239

п р и к а з ы в а ю:

1. Утвердить Правила выявления инцидентов, которые могут привести к сбоям или нарушению функционирования государственных информационных систем и объектов критической информационной инфраструктуры Ленинградской области и

(или) к возникновению угроз безопасности информации, и реагирования на них (приложение 1).

2. Утвердить форму Перечня лиц, ответственных за выявление инцидентов и реагирование на них (приложение 2).

3. Утвердить форму Перечня лиц, которым разрешены действия по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации (приложение 3).

4. Контроль за исполнением настоящего приказа возложить на первого заместителя председателя Комитета цифрового развития Ленинградской области – начальника департамента информационной безопасности и инфраструктуры.

И.о. председателя
Комитета цифрового развития
Ленинградской области Д.В. Золков

УТВЕРЖДЕНО
приказом Комитета
цифрового развития
Ленинградской области
от 24 сентября 2020 года № 19
(приложение № 1)

Правила
выявления инцидентов, которые могут привести к сбоям или нарушению функционирования государственных информационных систем и объектов критической информационной инфраструктуры Ленинградской области и (или) к возникновению угроз безопасности информации, и реагирования на них

1. Основные положения

1.1. Настоящие Правила выявления инцидентов, которые могут привести к сбоям или нарушению функционирования государственных информационных систем и объектов критической информационной инфраструктуры Ленинградской области и (или) к возникновению угроз безопасности информации, и реагирования на них (далее – Правила), устанавливают порядок действий лиц, ответственных за обеспечение информационной безопасности, администраторов и пользователей государственных информационных систем (ГИС), центра обработки данных (ЦОД) и единой сети передачи данных Ленинградской области (ЕСПД) при обнаружении событий и инцидентов информационной безопасности (далее – инцидент) и реагировании на них.

1.2. Основные понятия и определения.

Событие информационной безопасности - идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политик информационной безопасности (ИБ) или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности.

Инцидент информационной безопасности - появление одного или нескольких нежелательных или неожиданных событий ИБ, с которыми связана значительная вероятность компрометации работы ГИС, ЦОД или ЕСПД, и создания угрозы ИБ.

1.3. Правила включают в себя процессы:

– обнаружение и сообщение о возникновении событий ИБ (человеком или

автоматическими средствами);

– сбор информации, связанной с событиями ИБ, и оценка этой информации с целью определения, какие события можно отнести к категории инцидентов ИБ;

– реагирование на инциденты ИБ.

2. Обнаружение и сообщение о возникновении событий ИБ

2.1. К источникам обнаружения событий ИБ относятся сообщения пользователей, администраторов, ответственных за ИБ, уполномоченных федеральных органов исполнительной власти, иных организации, оповещения систем и сервисов работы и обеспечения безопасности ГИС, ЦОД, ЕСПД о событиях ИБ (далее - источники)

2.2. Пользователи, администраторы, ответственные за ИБ, уполномоченные федеральные органы исполнительной власти, иные организации (далее - участники событий ИБ) при возникновении событий ИБ, направляют информацию согласно приложению 1 в отдел информационной безопасности Комитета цифрового развития Ленинградской области (далее - отдел ИБ).

3. Сбор и оценка информации, связанной с событиями ИБ

3.1. Отдел ИБ ведет сбор информации, связанной с событиями ИБ и оценку этой информации с целью отнесения событий ИБ к инцидентам ИБ, во взаимодействии с участниками событий ИБ.

4. Реагирование на инциденты ИБ

4.1. Пользователи при обнаружении событий ИБ обязаны выполнить следующие действия:

выключить автоматизированное рабочее место из сети электропитания;

сообщить ответственному за ИБ (при его наличии) и в отдел ИБ;

выполнять указания ответственного за ИБ, специалистов отдела ИБ, администраторов и службы технической поддержки, в рамках устранения инцидента ИБ.

4.2. Администраторы и ответственные за ИБ при обнаружении инцидентов ИБ, и в целях недопущения инцидентов ИБ, предоставляют информацию

запрашиваемую отделом ИБ и выполняют указания отдела ИБ в рамках устранения инцидента ИБ.

4.3. Отдел ИБ:

проводит первоначальный анализ полученных данных о событии ИБ;

принимает решение о действиях по реагированию на инцидент ИБ.

Приложение 1 к Правилам выявления инцидентов, которые могут привести к сбоям или нарушению функционирования государственных информационных систем и объектах критической информационной инфраструктуры Ленинградской области и (или) к возникновению угроз безопасности информации, и реагирования на них

Информация о событии ИБ

Должность, фамилия и имя лица, сообщившего о событии ИБ	
Контактная информация (телефон, адрес электронной почты)	
Дата и время обнаружения инцидента	
Описание обнаруженного события или инцидента ИБ (характер воздействия, описание объектов, вовлеченных в инцидент, источник воздействия, наличие лог-файлов, и другие сведения об инциденте)	*Указывается событие или инцидент ИБ в свободной форме, например:* *заражение вредоносным программным обеспечением;* *распространение вредоносного программного обеспечения;* *нарушение или существенное замедление работы информационного ресурса;* *несанкционированный доступ или попытки несанкционированного доступа в систему;* *сбор сведений с использование ИКТ;* *организационные нарушения безопасности информации;* *распространение информации с неприемлемым содержимым;* *мошенничество с использованием ИКТ;* *уязвимость.*

УТЕРЖДЕНО
приказом Комитета
цифрового развития
Ленинградской области
от 24 сентября 2020 года № 19
(приложение № 2)

Форма
перечня лиц, ответственных за выявление инцидентов и реагирование на них

ФИО	Должность	Область ответственности

УТВЕРЖДЕНО
приказом Комитета
цифрового развития
Ленинградской области
от 24 сентября 2020 года № 19
(приложение № 3)

Форма
перечня лиц, которым разрешены действия по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации

ФИО	Должность	Разрешенные действия