ПРАВИТЕЛЬСТВО АЛТАЙСКОГО КРАЯ

ПОСТАНОВЛЕНИЕ

19.11.2020 № 497

г. Барнаул

Об утверждении Порядка взаимодействия органов исполнительной власти Алтайского края с Министерством цифрового развития и связи Алтайского края в части реагирования на инциденты информационной безопасности

В соответствии с Положением о системе защиты информации в органах исполнительной власти Алтайского края, утвержденным постановлением Правительства Алтайского края от 08.09.2017 № 336, Положением о Министерстве цифрового развития и связи Алтайского края, утвержденным указом Губернатора Алтайского края от 06.12.2018 № 194, в целях совершенствования системы защиты информации в органах исполнительной власти Алтайского края, обеспечения информационной безопасности и организации порядка реагирования на инциденты информационной безопасности Правительство Алтайского края п о с т а н о в л я е т:

1. Утвердить Порядок взаимодействия органов исполнительной власти Алтайского края с Министерством цифрового развития и связи Алтайского края в части реагирования на инциденты информационной безопасности (приложение).

2. Органам исполнительной власти Алтайского края назначить администраторов информационной безопасности, ответственных за обеспечение взаимодействия с Министерством цифрового развития и связи Алтайского края в части реагирования на инциденты информационной безопасности в органах исполнительной власти Алтайского края и подведомственных им учреждениях.

Губернатор Алтайского края,
Председатель Правительства
Алтайского края В.П. Томенко

Правительство Алтайского края
ДЛЯ ДОКУМЕНТОВ

ПРИЛОЖЕНИЕ

УТВЕРЖДЕН
постановлением Правительства Алтайского края
от 19.11. 2020 № 497

ПОРЯДОК
взаимодействия органов исполнительной власти Алтайского края с Министерством цифрового развития и связи Алтайского края в части реагирования на инциденты информационной безопасности

1. Общие положения

1.1. Порядок взаимодействия органов исполнительной власти Алтайского края с Министерством цифрового развития и связи Алтайского края в части реагирования на инциденты информационной безопасности (далее – «Порядок») устанавливает последовательность действий при возникновении угроз информационной безопасности, обусловленных возможностью несанкционированного доступа к государственным информационным системам и ресурсам сторонних лиц (третьих лиц), внедрения и распространения вредоносного программного обеспечения, проведения вирусных и сетевых атак, а также возможными техническими сбоями в работе программного и аппаратного обеспечения в части взаимодействия с Министерством цифрового развития и связи Алтайского края (далее – «уполномоченный орган»).

1.2. Настоящий Порядок разработан в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Положением о системе защиты информации в органах исполнительной власти Алтайского края, утвержденным постановлением Правительства Алтайского края от 08.09.2017 № 336, и иными нормативными правовыми актами Российской Федерации и Алтайского края в области защиты информации.

1.3. В настоящем Порядке используются следующие понятия:

инцидент информационной безопасности – появление одного или нескольких нежелательных или неожиданных событий информационной безопасности, с которыми связана значительная вероятность компрометации бизнес-процессов и создания угрозы информационной безопасности;

информационное взаимодействие – процесс обмена информацией между органами исполнительной власти Алтайского края и уполномоченным органом;

администратор информационной безопасности – должностное лицо, назначенное в органе исполнительной власти Алтайского края, ответственное за организацию защиты информации и взаимодействие с уполномоченным органом в части реагирования на инциденты информационной безопасности

в органах исполнительной власти Алтайского края и подведомственных им учреждениях.

участники информационного взаимодействия – органы исполнительной власти Алтайского края, уполномоченный орган.

2. Источники и виды инцидентов информационной безопасности

2.1. Источниками информации об инцидентах информационной безопасности в органах исполнительной власти Алтайского края являются:

сообщения о фактах выявления инцидентов информационной безопасности, полученные от сотрудников органов исполнительной власти и подведомственных им учреждений;

результаты работы средств мониторинга информационной безопасности, аудита (внутреннего или внешнего);

сообщения о выявленных инцидентах информационной безопасности, полученные от уполномоченного органа;

сообщения о выявленных инцидентах информационной безопасности, полученные от Управления Федеральной службы по техническому и экспортному контролю по Сибирскому федеральному округу, Управления Федеральной службы безопасности Российской Федерации по Алтайскому краю;

иные источники информации.

2.2. Основными видами инцидентов информационной безопасности в органах исполнительной власти Алтайского края являются:

попытка несанкционированного доступа к информационным системам и ресурсам;

компрометация учетных записей или паролей;

вирусная атака или вирусное заражение;

иные виды сетевых и вирусных атак, которые могут быть классифицированы как инциденты информационной безопасности.

3. Меры реагирования на инциденты информационной безопасности

3.1. При выявлении инцидента информационной безопасности в органах исполнительной власти Алтайского края и подведомственных им учреждениях администратор информационной безопасности обязан:

принять необходимые меры по устранению инцидента информационной безопасности;

принять меры по устранению причин возникновения инцидента информационной безопасности;

сохранить образ или содержание информационной системы или ресурса, в том числе журналы событий (информационного ресурса), на момент обнаружения инцидента информационной безопасности;

провести мероприятия по восстановлению работоспособности информационной системы (информационного ресурса);

провести проверку с целью выявления причин, которые могли привести к произошедшему инциденту информационной безопасности.

3.2. Администратор информационной безопасности органа исполнительной власти, подвергшегося несанкционированному воздействию, должен в течение одного рабочего дня с момента обнаружения несанкционированного воздействия представить в уполномоченный орган данные о факте возникновения инцидента информационной безопасности в виде карточки инцидента информационной безопасности по форме, представленной в приложении к настоящему порядку, а также в течение трех рабочих дней предоставить результаты проверки и информацию о последствиях инцидента информационной безопасности и принятых мерах по устранению его причин в форме письма в уполномоченный орган.

3.3. По результатам рассмотрения полученной информации об инцидентах информационной безопасности уполномоченным органом в течение двух рабочих дней принимается решение о достаточности либо недостаточности принятых мер и необходимости информирования Управления Федеральной службы по техническому и экспортному контролю по Сибирскому федеральному округу, Управления Федеральной службы безопасности Российской Федерации по Алтайскому краю о факте инцидента информационной безопасности. В случае принятия решения о недостаточности принятых мер уполномоченный орган собирает оперативное совещание с представителями органа исполнительной власти, подвергшегося несанкционированному воздействию, с целью выработки мер по устранению инцидента информационной безопасности.

4. Обязанности участников информационного взаимодействия

4.1. Уполномоченный орган обязан обеспечивать доведение до органов исполнительной власти Алтайского края и подведомственных им учреждений информационных сообщений и методических рекомендаций Управления Федеральной службы по техническому и экспортному контролю по Сибирскому федеральному округу, Управления Федеральной службы безопасности Российской Федерации по Алтайскому краю в области обеспечения защиты информации.

4.2. Обязанностями органов исполнительной власти Алтайского края в части реагирования на инциденты информационной безопасности являются:

организация работы по выявлению инцидентов информационной безопасности в органах исполнительной власти Алтайского края и подведомственных им учреждениях;

принятие необходимых мер по реагированию на инциденты информационной безопасности в соответствии с пунктами 3.1 и 3.2 настоящего Порядка;

принятие информационных сообщений от уполномоченного органа об организации дополнительных работ по профилактике инцидентов ин-

формационной безопасности и обеспечению защиты информации в органах исполнительной власти Алтайского края и подведомственных им учреждениях;

предоставление в уполномоченный орган актуальных контактных данных администраторов информационной безопасности (фамилия, имя, отчество, должность, номер служебного телефона, адрес служебной электронной почты).

ПРИЛОЖЕНИЕ
к Порядку взаимодействия органов исполнительной власти Алтайского края с Министерством цифрового развития и связи Алтайского края в части реагирования на инциденты информационной безопасности

ФОРМА
карточки инцидента информационной безопасности

Информационные ресурсы, на которых зафиксирован инцидент

Информация/данные (наименование информационной системы, сетевое имя и IP-адрес машины, сетевое имя и IP-адрес хост-машины (при наличии):_____

_____

_____

Дата и время обнаружения инцидента:_____

Описание события информационной безопасности

_____

_____

_____

_____

_____

_____

Принятые меры по устранению инцидента информационной безопасности:

_____

_____

_____

_____

_____

Информация о сообщающем лице (администраторе информационной безопасности):

Ф.И.О.:_____

Должность:_____

Организация:_____

_____

Телефон, e-mail:_____