М16

УТВЕРЖДАЮ
Председатель
Кооператива ЖКС «Энергетик»
Золотов Ю.Ю. Золотов
«09» января 2018 г.

Порядок реагирования на инциденты информационной безопасности в Кооперативе ЖКС «Энергетик»

2018 г.

1. Общие положения

1.1. Настоящий Порядок реагирования на инциденты информационной безопасности Кооператива ЖКС «Энергетик» определяет единый порядок реагирования на инциденты информационной безопасности, проведения служебных расследований, а также проведения мероприятий по предотвращению повторных инцидентов в Кооперативе ЖКС «Энергетик» (далее – Кооператив).

1.2. К инцидентам информационной безопасности относятся:

– разглашение информации ограниченного распространения;
– передача защищаемой информации по открытым каналам связи;
– обработка защищаемой информации на незащищенных технических средствах обработки информации;
– опубликование защищаемой информации в средствах массовой информации;
– передача носителя защищаемой информации лицу, не имеющему права доступа к ней;
– утрата или хищение носителя с защищаемой информацией;
– несанкционированное изменение защищаемой информации;
– несанкционированное копирование защищаемой информации;
– использование закладочных устройств и программных закладок;
– применение программных вирусов;
– неконтролируемые изменения в информационной системе;
– нарушение функционирования технических средств обработки информации, в том числе дефекты, сбои, отказы, аварии технических средств;
– дефекты, сбои, отказы в работе программного обеспечения.

1.3. К контролируемым инцидентам также относятся:

- сеансы работы в информационной системе персональных данных незарегистрированных пользователей;
- сеансы работы пользователей информационной системы персональных данных, срок действия полномочий, которых истек, либо в состав полномочий, которых не входят выявленные действия с персональными данными;
- действия третьего лица, пытающегося получить (или получившего) доступ к персональным данным с использованием учетной записи другого пользователя методом подбора пароля или иными методами (случайного разглашения пароля и т.п.) без ведома владельца учетной записи;
- совершение попыток несанкционированного доступа к рабочей станции, сейфу, шкафу и др. (нарушение целостности пломб, наклеек с защитной и идентификационной информацией, нарушение или несоответствие номеров печатей и др.);
- несанкционированное внесение изменений в параметры конфигурации программных или аппаратных средств обработки, или защиты, входящих в состав информационной системы персональных данных.

2. Оповещение об инциденте информационной безопасности

2.1. В случае обнаружения инцидента информационной безопасности сотрудник обязан:

- прекратить работу с ресурсом, в котором выявлен инцидент;
- оповестить своего непосредственного руководителя и должностное лицо, ответственное за защиту персональных данных, и предоставить им всю необходимую информацию по инциденту.

2.2. Должностное лицо, ответственное за защиту персональных данных, проводит анализ произошедшего инцидента информационной безопасности, причин, способствовавших его возникновению, и составляет служебную записку. Служебная записка должна содержать

описание инцидента, оценку его последствий и рекомендации о проведении в случае необходимости служебной проверки.

2.3. Служебная записка представляется председателю Кооператива для принятия решения о проведении служебной проверки инцидента информационной безопасности.

2.4. В случае если инцидент информационной безопасности стал (либо может стать) причиной возникновения негативных последствий для субъектов персональных данных, должностное лицо, ответственное за защиту персональных данных, обязано немедленно блокировать персональные данные этих субъектов до устранения причин инцидента.

3. Проведение служебной проверки инцидента информационной безопасности

3.1. Служебная проверка в обязательном порядке назначается в случае выявления:

- нарушения конфиденциальности, целостности или доступности персональных данных;
- несоблюдения требований по обеспечению безопасности персональных данных;
- несоблюдения условий хранения носителей персональных данных;
- использования средств защиты информации, которые могут привести к нарушению заданных характеристик безопасности или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

3.2. Служебная проверка проводится в целях:

- установление обстоятельств нарушения, в том числе времени, места и способа его совершения;
- установление лиц, виновных в данном нарушении;
- выявление причин и условий, способствовавших нарушению.

3.3. Служебная проверка назначается приказом председателя Кооператива, который образует комиссию, в состав которой включаются должностное лицо, ответственное за защиту персональных данных, администратор информационной безопасности и иные сотрудники Кооператива.

3.4. Комиссия должна приступить к работе не позднее следующего рабочего дня после даты выявления инцидента информационной безопасности.

Общая продолжительность служебной проверки не должна превышать десяти рабочих дней.

3.5. В случае если служебная проверка назначена в отношении конкретного сотрудника Кооператива, он должен быть ознакомлен с приказом о назначении проверки под роспись и представить письменные объяснения. Если по истечении двух рабочих дней указанные объяснения сотрудником не представлены, то комиссией составляется соответствующий акт.

3.6. По окончании служебной проверки комиссия представляет председателю Кооператива отчет, который должен содержать:

- основания и срок проведения проверки;
- время, место и обстоятельства нарушения;
- причины и условия совершения нарушения;
- виновные лица и степень их вины;
- наличие умысла в действиях виновных лиц;
- предложения по возмещению ущерба;
- предлагаемые взыскания или иные действия;
- рекомендации по исключению подобных нарушений в дальнейшем;
- другие вопросы, поставленные перед комиссией.

3.7. К отчету прилагаются:

- письменные объяснения сотрудников Учреждения;
- акты (справки) проверок носителей конфиденциальной информации, осмотров помещений и т.д.;
- иные относящиеся к проверке документы.

3.8. Отчет должен быть подписан всеми членами комиссии. При несогласии с выводами или содержанием отдельных положений отчета член комиссии вправе приобщить к нему свое особое мнение.

3.9. Отчет подлежит утверждению председателем Кооператива.

При выявлении по результатам проверки совершения сотрудником дисциплинарного проступка к нему может быть применено дисциплинарное взыскание в соответствии с Трудовым кодексом РФ.

При наличии в действиях сотрудника признаков административного правонарушения или уголовного преступления председатель Кооператива обязан обратиться в правоохранительные органы для привлечения виновного к ответственности, в соответствии с действующим законодательством.

3.10. Возмещение причиненного сотрудником ущерба производится в соответствии с Трудовым кодексом РФ.

3.11. Материалы служебной проверки инцидента информационной безопасности подшиваются в отдельное дело, которое хранится у должностного лица Кооператива, ответственного за организацию работ по обработке персональных данных.

4. Превентивные меры по недопущению повторного возникновения инцидентов информационной безопасности

4.1. В целях предупреждения и повторения инцидентов информационной безопасности в Кооперативе осуществляются:

- мониторинг событий в информационной системе персональных данных;
- своевременное удаление неиспользуемых учетных записей;
- контроль и мониторинг действий пользователей в информационной системе персональных данных;
- проведение обучения (повторного обучения) пользователей правилам обработки и обеспечения безопасности персональных данных.