Приложение № 1

к распоряжению администрации Красночетайского района

Чувашской Республики

от 24 .01. 2017 № 29

Регламент выявления инцидентов информационной безопасности и реагирования на них в администрации Красночетайского района

Чувашской Республики

**1. Общие положения**

* 1. Настоящий Регламент разработан в целях организации работы с инцидентами информационной безопасности (далее ‑ инцидент) в администрации Красночетайского района Чувашской Республики (далее – администрация района).
	2. Инцидент - одно событие или группы событий, которые могут привести к сбоям или нарушению функционирования информационной системы (далее - ИС) и (или) к возникновению угроз безопасности информации, в том числе персональных данных.
	3. Регламент выявления инцидентов информационной безопасности и реагирования на них в администрации Красночетайского района Чувашской Республики (далее - Регламент) разработано в соответствии с:
1. Федеральным законом Российской Федерации от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации";
2. Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ "О персональных данных";
3. требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119;
4. требованиями по реализации мер, предусмотренных составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утверждёнными приказом ФСТЭК России от 18 февраля 2013 года № 21;
5. политикой информационной безопасности администрации района.
	1. Работа с инцидентами в области информационной безопасности помогает определить наиболее актуальные угрозы информационной безопасности и создает обратную связь в системе обеспечения информационной безопасности, что способствует повышению общего уровня защиты информационных ресурсов и информационных систем.
	2. Работа с инцидентами включает в себя следующие направления:
6. определение лиц, ответственных за выявление инцидентов и реагирование на них;
7. обнаружение, идентификация и регистрация инцидентов;
8. своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами;
9. анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а так же оценка их последствий;
10. принятие мер по устранению последствий инцидентов;
11. планирование и принятие мер по предотвращению повторного возникновения инцидентов.
	1. Примерный перечень инцидентов информационной безопасности приведен в приложении № 1 к настоящему Регламенту.
12. **Ответственные за выявление инцидентов и реагирование на них**
	1. Ответственными за выявление инцидентов в ИС являются:
13. лица, имеющие право доступа к ИС;
14. ответственный за техническое обслуживание ИС;
15. администратор ИС;
16. администратор информационной безопасности ИС.
	1. Ответственными за реагирование на инциденты в ИС являются:
17. лица, имеющих право доступа к ИС;
18. руководитель подразделения администрации района, в котором выявлен инцидент;
19. ответственный за техническое обслуживание ИС;
20. администратор ИС;
21. администратор информационной безопасности ИС;
22. ответственный за организацию обработки персональных данных в администрации района в случае, если ИС является информационной системой персональных данных (далее - ИСПДн);
23. **Обнаружение, идентификация и регистрация инцидентов**
	1. Работа по идентификации инцидентов в области информационной безопасности включает в себя мероприятия, направленные на доведение до сотрудников администрации района информации, позволяющей идентифицировать инциденты.
	2. В качестве источников информации об инцидентах информационной безопасности могут использоваться:

электронные журналы и оповещения системного и прикладного программного обеспечения информационных систем администрации района;

электронные журналы и оповещения системы защиты информации (далее ‑ СЗИ);

оповещения средств обнаружения вторжений;

информация, получаемая от сотрудников;

информация, полученная на основе анализа защищенности ИС и контроля эффективности СЗИ.

* 1. В информационных системах администрации района в обязательном порядке должны регистрироваться следующие события безопасности:

попытки входа (выхода) пользователей в операционную систему (из операционной системы);

загрузка и инициализация операционной системы и ее программного останова для рабочих станций и серверов;

попытка доступа к средствам виртуализации;

факт изменения конфигурации средств виртуализации;

запуск и остановка служб (системных сервисов) средств виртуализации;

попытки подключения к серверам и рабочим станциям по информационно-телекоммуникационной сети;

попытки подключения к серверам и рабочим станциям мобильных устройств и внешних носителей информации.

* 1. В параметрах регистрации событий безопасности в обязательном порядке должны указываться следующие параметры:

тип события;

дата и время события;

результат события;

источник события;

идентифицирующие сведения (сетевой адрес, данные учетной записи, сетевое имя компьютера, и т.п.).

* 1. Хранение электронных журналов регистрации и учета событий безопасности операционных систем, систем управления базами данных, системного и прикладного программного обеспечения, средств защиты информации, а также специализированных средств анализа защищенности информационных систем должно осуществляться в течение срока, достаточного для проведения анализа инцидента, но не менее 3 месяцев.
	2. Хранение электронных журналов регистрации и учета событий безопасности должно осуществляться администратором информационной безопасности администрации района с учетом требований обеспечения конфиденциальности и целостности электронных журналов.
	3. Учет инцидентов осуществляется администратором информационной безопасности администрации района, в соответствии с формой журнала учета инцидентов информационной безопасности в администрации района, приведенной в приложении № 2 к настоящему Регламенту.
1. **Информирование о возникновении инцидентов**

4.1. Сотрудник администрации района (пользователь ИС), обнаруживший инцидент в ИС, должен незамедлительно, любым доступным способом, сообщить об инциденте непосредственному руководителю, администратору ИС, администратору информационной безопасности ИС, ответственному за организацию обработки персональных данных в администрации района (в случае если ИС является ИСПДн).

4.2. Администратор ИС, в случае необходимости, информирует пользователей ИС о возникновении инцидента и дает указания по дальнейшим действиям.

1. **Анализ инцидентов, а также оценка их последствий**
	1. Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценки их последствий, осуществляет постоянно действующая техническая комиссия.
	2. Источниками и причинами возникновения инцидентов в области информационной безопасности являются:
2. действия организаций и отдельных лиц враждебные интересам администрации района;
3. отсутствие персональной ответственности сотрудников администрации и их руководителей за обеспечение информационной безопасности, в том числе персональных данных;
4. недостаточная работа с персоналом по обеспечению необходимого режима соблюдения конфиденциальности, в том числе персональных данных;
5. отсутствие дисциплинарной мотивации соблюдения правил и требований информационной безопасности;
6. недостаточная техническая оснащённость подразделений, ответственных за обеспечение информационной безопасности;
7. совмещение функций по разработке и сопровождению или сопровождению и контролю за информационными системами;
8. наличие привилегированных бесконтрольных пользователей в информационной системе;
9. пренебрежение правилами и требованиями информационной безопасности сотрудниками администрации района;
10. и другие причины.
	1. В ходе анализа инцидента определяются:

категория инцидента;

факт или потенциальная возможность реализации угрозы безопасности защищаемой информации (далее ‑ угрозы);

опасность угрозы;

области, перечни информационных ресурсов, затрагиваемые воздействием угрозы;

потенциальные нарушители, цели и причины реализации угрозы;

предварительный перечень мер по локализации и остановке распространения действия угрозы.

* 1. Оценка последствий инцидента производится на основании потенциально возможного или фактического ущерба.
1. **Принятие мер по устранению последствий инцидентов**

Меры по устранению последствий инцидентов включает в себя мероприятия, направленные на:

1. определение границ инцидента и ущерба от реализации угроз информационной безопасности;
2. ликвидацию последствий инцидента и полное либо частичное возмещение ущерба.
3. **Планирование и принятие мер по предотвращению инцидентов**
4. Планирование и принятие мер по предотвращению возникновения инцидентов осуществляет постоянно действующая техническая комиссия и основывается на:
5. планомерной деятельности по повышению уровня осознания информационной безопасности руководством и сотрудниками администрации района;
6. проведении мероприятий по обучению сотрудников администрации района правилам и способам работы со средствами защиты информационных систем;
7. доведении до сотрудников норм законодательства, внутренних документов администрации района, устанавливающих ответственность за нарушение требований информационной безопасности;
8. разъяснительной работе с увольняющимися сотрудниками и сотрудниками, принимаемыми на работу;
9. своевременной модернизации системы обеспечения информационной безопасности, с учетом возникновения новых угроз информационной безопасности, либо в случае изменения требований руководящих документов по организации обеспечения информационной безопасности;
10. своевременном обновлении программного обеспечения, в том числе баз сигнатур антивирусных средств.
11. Работа с персоналом.

Как правило, самым слабым звеном в любой системе безопасности является человек. Поэтому работа с персоналом является основным направлением деятельности по обеспечению требований информационной безопасности.

Персонал администрации района является важным источником сведений об инцидентах информационной безопасности, поэтому необходимо донести до сотрудников информацию о том, что оперативно предоставленные сведения об инциденте информационной безопасности являются основанием для смягчения либо отмены наказания за нарушение требований информационной безопасности.

Приложение № 1

к Регламенту выявления инцидентов информационной безопасности и реагирования на них в администрации Красночетайского района Чувашской Республики

**Примерный перечень
инцидентов информационной безопасности**

| **№** **п/п** | **Описание инцидента информационной безопасности** |
| --- | --- |
| **Инциденты категории 1** |
|  | Однократные ошибки при регистрации пользователя информационной системы, связанные в вводом неверных регистрационных данных (пароля, имени пользователя и т.п.) более пяти раз подряд, приводящие к блокировке учетных данных пользователей |
|  | Однократные попытки неудачного доступа к объектам (серверам, телекоммуникационному оборудованию, средствам защиты информации, компьютерам, принтерам, файлам)  |
|  | Несанкционированный перевод времени на рабочей станции, либо на других элементах информационной инфраструктуры  |
|  | Оставление работающего (включенного) компьютера без блокировки экрана в рабочее время (при отсутствии сотрудника на рабочем месте) |
|  | Перезагрузка рабочей станции при сбоях в работе технических или программных средств. |
|  | Нецелевое использование сотрудниками элементов информационной инфраструктуры (печать, сервисы сети Интернет, электронная почта, и т.п.) |
| **Инциденты категории 2** |
|  | Регулярные попытки неудачного доступа к объектам (серверам, телекоммуникационному оборудованию, средствам защиты информации, компьютерам, принтерам, файлам)  |
|  | Ошибки при регистрации администратора информационной системы, связанные с вводом неверных регистрационных данных (пароля, имени пользователя и т.п.) более пяти раз подряд, приводящие к блокировке учетных данных администратора |
|  | Многократные ошибки при регистрации пользователя в информационной системе (повторяющиеся случаи ввода неправильных регистрационных данных (пароля, имени пользователя и т.п.) более 5 раз подряд, приводящие к блокировке учетных данных пользователей) |
|  | Неоднократное оставление работающего (включенного) компьютера без блокировки экрана в рабочее время (при отсутствии сотрудника на рабочем месте) |
|  | Выход из строя или утрата носителя информации с резервной копией баз данных или учтенного носителя конфиденциальной информации |
|  | Неудачные попытки регистрации в информационной системе под чужими регистрационными данными (именем пользователя, паролем и т.п.)  |
|  | Регистрация в информационной системе под чужими регистрационными данными (именем пользователя, паролем и т.п.) |
|  | Регистрация или попытки регистрации в информационной системе с учетными данными пользователя, которые не соответствуют штатным зарегистрированным техническим средствам и сетевым идентификационным данным (адресам) пользователя |
|  | Нерегламентированная очистка электронных журналов событий безопасности информационных систем и потеря их целостности |
|  | Нерегламентированное подключение неучтенных внутренних и (или) периферийных устройств и носителей информации |
|  | Нерегламентированное изменение аппаратной конфигурации серверного оборудования или технических средств рабочей станции |
|  | Перезагрузка сервера при сбоях в работе, которая может привести к нарушению работы системного или прикладного программного обеспечения или нарушению целостности и доступности информации (баз данных) |
|  | Нерегламентированное копирование информации (файлов) на флеш-накопители или иные внешние носители информации, а также нерегламентированная передача подобной информации с использованием сервисов электронной почты, мгновенных сообщений (ICQ и т.п.) и других сервисов сети Интернет |
|  | Нерегламентированная установка (удаление) прикладного программного обеспечения, не разрешенного к использованию на рабочих станциях и серверах |
|  | Попытка получения привилегированного доступа к рабочей станции или к другим ресурсам информационных систем (повышение уровня прав доступа, получение прав на отладку программ и т.п.) |
|  | Заражение программного обеспечения рабочих станций и серверов вредоносным кодом (непреднамеренное) |
|  | Использование сканирующего (на различные уязвимости) программного обеспечения |
|  | Использование анализаторов протоколов (снифферов) |
|  | Попытки реализации сетевых атак на информационно-телекоммуникационную инфраструктуру и информационные ресурсы, совершаемых с использованием внешних информационно-телекоммуникационных сетей, в том числе атак типа «отказ в обслуживании» (DDoS-атака) |
|  | Нерегламентированный просмотр, вывод на печать, передача третьим лицам сведений, содержащих конфиденциальные данные (информацию, подлежащую защите) |
|  | Несанкционированное проведение обновления версий системного и прикладного программного обеспечения |
| **Инциденты категории 3** |
|  | Несанкционированное получение привилегированного доступа к любым элементам информационной инфраструктуры |
|  | Несанкционированное изменение конфигурации элементов информационной инфраструктуры |
|  | Хищение носителей резервных копий баз данных |
|  | Утечка конфиденциальной информации (баз данных информационных систем и др.) |
|  | Подозрение в умышленном нарушении работоспособности информационной сети, элементов информационной инфраструктуры, системного и прикладного программного обеспечения  |
|  | Несанкционированная передача (распространение) конфиденциальной информации  |
|  | Несанкционированное внесение изменений в базы данных информационных систем |
|  | Несанкционированное уничтожение конфиденциальной информации |
|  | Проведение технического обслуживания (ремонт) или изменение в характеристик и конфигурации информационных систем, повлекшее за собой потерю конфиденциальной информации |
|  | Намеренное заражение информационных систем вредоносным программным обеспечением |

приложение № 2

к Регламенту выявления инцидентов информационной безопасности и реагирования на них в администрации Красночетайского района Чувашской Республики

**Форма журнала учета инцидентов информационной безопасности**

**в администрации Красночетайского района Чувашской Республики**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Дата** | **Описание инцидента, категория** | **Источник получения информации об инциденте** | **Принятые меры** | **ФИО ответственного за управление инцидентами**  | **Подпись ответственного за управление инцидентами** | **Подпись ответственного за обеспечение безопасности** |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 7 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

ЛИСТ ОЗНАКОМЛЕНИЯ

с распоряжением администрации Красночетайского района Чувашской Республики

от 24.01.2017 № 29 «О регламенте выявления инцидентов информационной безопасности и реагирования на них в администрации Красночетайского района Чувашской Республики»

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №п.п. | ФИО | Должность | Личная подпись | Дата |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |