ИНСТРУКЦИЯ
О ПОРЯДКЕ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ ПО РЕАГИРОВАНИЮ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ВО ВНЕШТАТНЫХ (КРИЗИСНЫХ) СИТУАЦИЯХ

Астана
2023 год

Термины и сокращения

Организация – ОЮЛ Ассоциация ВИЭ «Qazaq Green»;

Инструкция – Инструкция о порядке действий пользователей по реагированию на инциденты информационной безопасности и во внештатных (кризисных) ситуациях Организации.

Компрометация пароля – утечка или разглашение пароля.

Несанкционированный доступ к информации (далее – НСД) – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Первый руководитель – Директор либо лицо, исполняющее его обязанности;

Провайдер – юридическое лицо (лица), оказывающее услуги по размещению оборудования специализированных информационных систем, подключению к сети Интернет и иные связанные с сопровождению систем услуги.

Специалист по информационной безопасности (далее – ИБ) – Работник Организации, обеспечивающий поддержку и развитие ИТ-инфраструктуры Организации.

Угроза - потенциальная причина нежелательного инцидента, который может нанести ущерб системе или Организации.

ПО – программное обеспечение.

ЛВС – локальная вычислительная сеть Организации.

Системный администратор (далее – СА) – работник, который выполняет функции администрирования серверов и прикладного активного оборудования корпоративной информационной сети, в соответствии с Должностными инструкциями системного администратора Организации.

1. Общие положения

1. Настоящая Инструкция определяет порядок действий пользователей корпоративной вычислительной сети, системного администратора, специалиста по информационной безопасности и административно-хозяйственных служб эксплуатации офиса при возникновении внештатных (кризисных) ситуаций в Организации.

2. В данной Инструкции в качестве внештатной ситуации рассматриваются:

1) длительное отсутствие связи с сервером;

2) сбой программного обеспечения, приводящий к невозможности дальнейшей обработки информации;

3) компрометация пароля;

4) выход из строя сервера или сетевого оборудования;

5) потеря или утечка информации на сервере или на персональном компьютере;

6) попытка НСД, зафиксированная средствами регистрации;

7) НСД к ИС или обнаружение злонамеренного кода в ПО;

8) выход из строя каналов связи;

9) нарушение подачи электроэнергии, приведшие к полной или частичной потере работоспособности ИС, к невозможности обработки информации средствами вычислительной техники Организации;

10) стихийные природно-климатические воздействия (землетрясение, наводнения, ураганы, пожары и т.д.);

11) иное воздействие на информационные ресурсы, приводящие к частичной потере работоспособности ИС (выходу из строя отдельных компонентов системы, потере производительности, нарушению целостности и конфиденциальности программ и информации) либо полному выходу ИС из строя (неспособности выполнять далее свои функции, уничтожению, блокированию, неправомерной модификации или компрометации информации).

3. Источниками информации о возникновении внештатной ситуации являются:

1) сообщение пользователей работнику отдела информационных технологий при обнаружении внештатной ситуации в работе аппаратно-программных комплексов ИС;

2) сообщение работников, осуществляющих эксплуатацию ИС, обнаруживших подозрительные изменения в работе или конфигурации системы, системному администратору и специалисту по информационной безопасности;

3) системы мониторинга состояния корпоративной информационной сети, серверов, пользовательских рабочих станций, ПО и пр.

4) системные журналы, в которых имеются записи, свидетельствующие о возникновении или возможности возникновения внештатной ситуации.

2. Общий порядок действий при возникновении внештатной ситуации

4. Пользователь, в случае возникновения внештатной ситуации, перечисленной в подпунктах 2, 3,5,6, 7, 10, 11 пункта 2 инструкции:

1) приостанавливает работу;

2) немедленно ставит в известность работника отдела информационных технологий;

3) информирует руководство;

4) возобновляет работу только после разрешения работника отдела информационных технологий по внештатным ситуациям, перечисленным в подпунктах 2, 9 пункта 2 и после разрешения специалиста по информационной безопасности по подпунктам 3,5,6,7,10, 11 пункта 2 инструкции.

5. Системный администратор проводит предварительный анализ ситуации, если возможно, оперативно устраняет и ставит в известность руководителя и фиксирует факт возникновения внештатной ситуации в журнале регистрации внештатных ситуаций (форма которого приведена в **Приложении 1** к настоящей Инструкции).

6. В случае возникновения внештатной ситуации, способной серьезно повлиять на осуществление бизнес-процессов Организации, работник отдела информационных технологий:

1) сообщает о возникновении внештатной ситуаций первому руководителю, а по внештатным ситуациям, перечисленным в подпунктах 3,5, 6,7,10,11 также специалисту по информационной безопасности;

2) определяет масштабы внештатной ситуации, размеры и область возможного поражения;

3) отключает пораженные компоненты или переключается на использование резервных ресурсов;

4) восстанавливает работоспособность поврежденных критичных аппаратных средств и другого оборудования, при необходимости производит замену отказавших узлов и блоков резервными;

5) восстанавливает поврежденное программное обеспечение, используя эталонные копии;

6) восстанавливает необходимую информацию, используя резервные копии;

7) проверяет работоспособность восстановленной системы, удостоверяется в том, что последствия внештатной ситуации не оказывают воздействия на дальнейшую работу системы;

8) уведомляет первого руководителя об устранении внештатной ситуации;

9) регистрирует внештатную ситуацию в журнале регистрации внештатных ситуаций.

10) предоставляет отчет о внештатной ситуации системному администратору.

7. Доступ к средствам вычислительной техники для установки и настройки программного обеспечения или замены сетевого оборудования имеет только работник отдела информационных технологий в соответствии с функциональными обязанностями.

8. Работником отдела информационных технологий, устранившим внештатную ситуацию, составляется акт с описанием ситуации.

9. Каждая внештатная ситуация анализируется специалистом по информационной безопасности. По результатам этого анализа вырабатываются и предоставляются руководству предложения по возможным организационным и техническим мероприятиям, направленным на предотвращение внештатных ситуаций в будущем.

10. При необходимости, по решению первого руководителя Организации, может быть проведено служебное расследование по факту возникновения внештатной ситуации, с целью выяснения её причин, оценки причиненного ущерба, определению виновных лиц и принятию соответствующих мер воздействия.

3. Контроль возникновения внештатных (кризисных) ситуаций и корректирующих действий по ним

11.Порядок оповещения должностных лиц и сроки выполнения мероприятий при внештатных ситуациях определены в Плане мероприятий по обеспечению непрерывной работы и восстановлению работоспособности активов, связанных со средствами обработки информации.

12.Для выполнения профилактических действий, с целью предотвращения возникновения внештатных или кризисных ситуаций должны проводиться следующие мероприятия:

1) Системный администратор должен ежедневно проводить мониторинг информационных систем Организации, включающий в себя опрос состояния СУБД, ОС и ППО, с помощью специализированного программного обеспечения, в случае изменения состояния доступности информационных систем произойдет оповещение администратора в режиме «онлайн»;

2) Системный администратор должен ежедневно проводить мониторинг событий, связанных с нарушением ИБ, и анализ результатов мониторинга;

3) Системный администратор должен проводить резервное копирование информации в соответствии с регламентом резервного копирования и восстановления информации;

4) В случаях получения информации о возможных предстоящих внештатных ситуациях, должно быть обеспечено оперативное оповещение всех причастных лиц и структур.

5) Системный администратор обязан как можно быстрее сообщать о любых событиях в сфере информационной безопасности Специалисту по информационной безопасности и произвести соответствующую запись возникновения внештатных ситуаций в документе «Журнал учета внештатных ситуаций», указанном в Приложении 1;

6) каждая внештатная ситуация должна анализироваться специалистом по информационной безопасности совместно с системным администратором.

13.Осуществление контроля, за выполнением профилактических действий для предотвращения возникновения внештатных или кризисных ситуаций возлагается на системного администратора.

14. Представитель руководства СУИБ является ответственным лицом за оповещение работников Организации в случае возникновения внештатных (кризисных) ситуаций и инцидентов информационной безопасности.

15.Для эффективной реализации мероприятий по реагированию в случае внештатных ситуаций должны проводиться регулярные тренировки по различным внештатным ситуациям. По результатам тренировки в случае необходимости проводится уточнение настоящей Инструкции.

16.Сбор, сохранение и предоставление информации об инцидентах информационной безопасности на случай, если инцидент информационной безопасности может привести к судебному разбирательству в соответствии с разделом 13.2.3 СТ РК ИСО МЭК 27002-2009

17.Регистрация событий, связанных с состоянием информационной безопасности и выявление нарушений путем анализа журналов событий в соответствие с Едиными Требованиями Республики Казахстан.

4. Особенности действий при возникновении наиболее распространенных внештатных ситуаций

18. При отсутствии связи с одним или несколькими серверами, расположенными у Провайдера, системным администратором немедленно проводится выяснение причин отсутствия связи и далее, при необходимости, проводятся мероприятия согласно настоящей Инструкции.

19.При сбое программного обеспечения работник отдела информационных технологий выясняет причину сбоя. Если исправить ошибку своими силами, в том числе после консультации с разработчиком программного обеспечения, не удалось, копия акта и сопроводительных материалов (а также файлов, если это необходимо) работником информационных технологий направляются разработчику программного обеспечения.

20. При компрометации пароля необходимо следовать Правилу по организации процедуры аутентификации Организации.

21. При обнаружении компьютерного вируса необходимо руководствоваться Правилами организации антивирусного контроля Организации.

22. При выходе из строя сервера или сетевого оборудования системный администратор должен:

1) отключить вышедшие из строя компоненты сервера или сетевого оборудования;

2) принять меры по немедленному вводу в действие резервного сервера или сетевого оборудования, при их наличии, для обеспечения непрерывной работы;

3) провести анализ на наличие потерь и/или нарушения целостности данных и программного обеспечения;

4) проверить работоспособность поврежденного оборудования;

5) восстановить работоспособность поврежденных компонентов или сервисов серверного, или сетевого оборудования (при необходимости восстановить программное обеспечение и данные из резервных копий с составлением акта).

23. В случае обнаружения потери или утечки информации на серверах или на персональных компьютерах пользователей, работником отдела информационных технологий в присутствии системного администратора проводятся мероприятия по поиску и устранению причин потери информации (проверка целостности и работоспособности ПО и средств вычислительной техники), при необходимости, восстанавливается информация из резервных копий. Если утечка информации произошла по техническим причинам, проводится анализ защищённости информации, принимаются меры по устранению и предотвращению возникновения уязвимостей.

24. При попытке НСД, зафиксированной средствами регистрации, системным администратором проводится анализ информации в журналах регистрации и по результатам анализа, в случае реальной угрозы НСД, принимаются следующие меры по предотвращению НСД:

1) проводится внеплановая полная смена паролей;

2) применяется имеющееся обновление программного обеспечения, устраняющее уязвимости системы безопасности.

25. При обнаружении НСД проводятся следующие мероприятия:

1) системным администратором и специалистом по информационной безопасности проводится оперативный анализ обстоятельств НСД, по результатам которого первым руководителем принимается решение о возможности продолжения эксплуатации ИС до завершения расследования инцидента.

2) при необходимости проводится отключении сервера от сети или остановка сервера для проверки ИС и ПО на наличие злонамеренного кода. Возможен временный переход на резервный сервер.

3) для последующего анализа средствами резервного копирования создается копия системы.

4) Системным администратором проводится анализ журналов регистрации сервера и журналов регистрации средств защиты информации.

5) проводится внеплановая смена паролей, которые имели отношение к серверам.

26. При выходе из строя каналов связи системный администратор ставит в известность поставщика услуг связи, отрабатывает вопрос восстановления канала связи, принимает меры по переходу на запасные каналы связи, в случае их наличия.

27. В случае отключения электроэнергии свыше 10 минут, и при невозможности использовать источники бесперебойного питания, работнику отдела информационных технологий необходимо провести корректное отключение всех серверов и сетевого оборудования. При подаче электроэнергии в здании Организации системный администратор совместно со специалистом по информационной безопасности проводят анализ на наличие потерь и (или) разрушения данных и ПО на сервере, также проверяют работоспособность оборудования. В случае необходимости, производится восстановление ПО и данных из последней резервной копии, с составлением акта.

28. При обнаружении отказа электропитания оборудования, расположенного в офисе или на территории Провайдера, работник информационных технологий немедленно ставит в известность уполномоченных работников. Если предполагаемое время устранения отказа электропитания превышает 30 минут, работник информационных технологий извещает первого руководителя. При возобновлении подачи электропитания

системным администратором проводятся мероприятия по проверке целостности оборудования и ПО.

29. При возникновении стихийного природно-климатического воздействия (землетрясение, наводнение, ураганы, пожары и т.д.) системные администраторы должен обеспечить по возможности сохранение последней полной копии системы.

30. Для выработки четких действий работников при стихийных бедствиях, специалист по информационной безопасности не менее одного раза в год должен организовывать обучающие специальные тренировки.

5. Средства обеспечения непрерывной работы и восстановления

31. В рамках данной Инструкции рассматриваются риски возникновения внештатных ситуаций технического характера.

Риски возникновения внештатных ситуаций техногенного воздействия и природных катаклизмов относятся к Чрезвычайным ситуациям и рассматриваются в документе: «Правила по обеспечению непрерывной работы активов, связанных со средствами обработки информации».

32. Средствами обеспечения непрерывной работы и восстановления является:

1) резервное копирование ПО и информационных ресурсов Организации;
2) источники бесперебойного питания на серверных машинах

33. Резервное копирование обеспечивает восстановление информации в случае потери информации. Резервное копирование выполняется в соответствии с требованиями Регламента проведения резервного копирования и восстановления информации.

34. Источники бесперебойного питания обеспечивают подключенному оборудованию некоторое время работы от аккумуляторов, в случае отключения или выхода параметров электрического тока за допустимые параметры.

6. Обязанности и действия персонала по обеспечению непрерывной работы и восстановлению информационных систем

35. Действия персонала в кризисной ситуации зависят от степени ее тяжести.

36.В случае возникновения угрожающей или серьезной критической ситуации действия персонала включают следующие этапы:

1) немедленная реакция ответственного персонала;
2) частичное восстановление работоспособности и возобновление обработки;
3) полное восстановление системы и возобновление обработки в полном объеме;
4) расследование причин возникновения кризисной ситуации и установление виновных;
5) в дневное время суток работник, обнаруживший внештатную (кризисную) ситуацию, должен поставить в известность своего непосредственного руководителя и системного администратора– устно, специалиста по информационной безопасности – устно, при необходимости, письменно;
6) выработка решений по устранению причин и недопущения в последующем подобных фактов нарушений.

37.Организация доводит до сведения организации, предоставляющей охрану здания, необходимость следующего: при возникновении внештатной ситуации в ночное время суток работник охраны ответственный за безопасность должен поставить в известность ответственного работника отела информационных технологий.

38.Работники, осуществляющие эксплуатацию ИС, обязаны извещать специалиста по информационной безопасности о всех замеченных предпосылках возникновения внештатных ситуаций.

39. Организацию работ в кризисных ситуациях осуществляют системный администратор и специалист по информационной безопасности, возложенных на них задач.

40. Контроль организации работ в кризисных ситуациях осуществляет руководитель Организации.

7. Контроль возникновения внештатных или кризисных ситуаций и корректирующих действий по ним

41. Контроль возникновения внештатных ситуаций осуществляется с помощью следующих функций:

1) регистрация возникновения внештатных ситуаций в журнале регистрации внештатных ситуаций;
2) составлением актов, с описанием внештатной ситуации и корректирующих действий, с приложением поясняющих материалов

(скриншотов, распечатки журнала событий и т.д.), зафиксированных документально, подтверждающих их подлинность.

8. Ответственность

42. Руководство и обслуживающий персонал, отвечающие за работоспособность ИС, несут ответственность за:

1) ненадлежащее выполнение своих функциональных обязанностей;

2) не обеспечение надлежащих условий сохранности, доступности, конфиденциальности обрабатываемой информации, в рамках своей компетенции.

43. Системный администратор не реже одного раза в полгода проводит анализ инцидентов, зафиксированных в журнале регистрации внештатных ситуаций, для разработки превентивных мер по снижению рисков появления повторных внештатных ситуаций.

44. Лица, нарушившие требования настоящей инструкции, привлекаются к дисциплинарной или иной ответственности в соответствии с действующим законодательством Республики Казахстан.

9. Контроль над соблюдением Инструкции

45. Контроль над соблюдением настоящей Инструкции осуществляет системный администратор и специалист по информационной безопасности.

46. За нарушение норм, предусмотренных настоящей Инструкцией, к работникам Организации по представлению специалиста по информационной безопасности, на основании материалов служебного расследования, могут быть применены меры дисциплинарного взыскания.

Приложение 1
к Инструкции о порядке действий пользователей по реагированию на инциденты информационной безопасности и во внештатных (кризисных) ситуациях

«__» _____ 202_ г. № __

Журнал регистрации внештатных ситуаций

№ п/п	Дата	Краткое описание нештатной ситуации	Время начала	Время окончания	Простой	Причина	Метод устранения	Ответственный

ЛИСТ ОЗНАКОМЛЕНИЯ

№	Фамилия, имя, отчество	Должность	Личная подпись	Дата
1	**2**	**3**	**4**	**5**
1				
2				
3				
4				
5				
6				
7				
8				
9				