МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МИРЭА – Российский технологический университет»

РТУ МИРЭА

Институт кибербезопасности и цифровых технологий

КБ-4 «Интеллектуальные системы информационной безопасности»

Отчет по практической работе №4.2 на тему: План Реагирования на компьютерные инциденты

по дисциплине: «Управление информационной безопасностью»

Выполнил:
Студент группы ББМО-01-22
ФИО: Карев Д.П.

Проверил:
Р. В. Пимонов

1. Нормативно-методическое обеспечение

Настоящий документ составлен в соответствии со следующими действующими нормативно-методическими документами по защите информации:

1. Положение о Национальном координационном центре по компьютерным инцидентам, утвержденное приказом ФСБ России от 24 июля 2018 г. № 366 "О Национальном координационном центре по компьютерным инцидентам".

2. Порядок ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденный приказом ФСТЭК России от 6 декабря 2017 г. № 227 "Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации".

3. Приказ ФСБ России от 19.06.2019 № 282 "Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации".

4. Приказ ФСТЭК России от 21.12.2017 года №235 (ред. от 27.03.2019) "Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования".

5. Приказ ФСТЭК России от 22.12.2017 года №236 (ред. от 21.03.2019) "Об утверждении формы направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий".

6. Приказ ФСТЭК России от 25.12.2017 года №239 (ред. 09.08.2018) (ред. 26.03.2019) "Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ".

7. Базовая модель угроз безопасности персональных данных при обработке, в информационных системах персональных данных (утверждена 15.02.2008 года заместителем директора ФСТЭК России).

8. Информационное сообщение ФСТЭК России от 04.05.2018 года №240/22/2339 "О методических документах по вопросам обеспечения безопасности информации в КСИИ РФ".

9. Информационное сообщение ФСТЭК России от 24.08.2018 года№240/25/3752 "По вопросам представления перечней объектов КИИ, подлежащих категорированию, и направления сведений о результатах присвоения объекту КИИ одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий".

10. Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 14.02.2008 года заместителем директора ФСТЭК России).

11. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности информации персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности (утверждены руководством 8 центра ФСБ России 31.03.2015 года № 149/7/2/6-432).

12. Методический документ ФСТЭК России "Методика определения угроз безопасности информации в информационных системах" (проект).

13. Методический документ ФСТЭК России от 11.02.2014 года "Меры защиты информации в государственных информационных системах".

14. Нормативно-методический документ ФСТЭК России от 30.08.2002 года "Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)", Гостехкомиссия России, 2002 год.

15. Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное приказом ФСБ России от 09.02.2005 года № 66 (зарегистрирован Минюстом России 03.03.2005, регистрационный № 6382).

16. Постановление Правительства РФ "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" от 01.11.2012 года № 1119.

17. Постановление Правительства РФ от 17.02.2018 года№162 "Об утверждении Правил осуществления госконтроля в области обеспечения безопасности значимых объектов КИИ РФ".

18. Постановление Правительства РФ от 13.04.2019 года №452 "О внесении изменений в постановление ПП-127 от 08.02.2018".

19. Постановление Правительства РФ от 08.06.2019 года №743 "Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов КИИ РФ".

20. Приказ ФСБ России от 06.05.2019 года №196 "Об утверждении требований к средствам ГосСОПКА.

Раздел 1. Технические характеристики и состав ЗОКИИ ФГБУ НПП ГАММА

Информация о технических характеристиках и составе ЗОКИИ Центра представлена в таблице 1.

Таблица 1. Технические характеристики и состав ЗОКИИ

Сведения о взаимодействии объекта критической информационной инфраструктуры и сетей электросвязи		
1.	Категория сети электросвязи (общего пользования, выделенная, технологическая, присоединенная к сети связи общего пользования, специального назначения, другая сеть связи для передачи информации при помощи электромагнитных систем) или сведения об отсутствии взаимодействия объекта критической информационной инфраструктуры с сетями электросвязи	Общего пользования
2.	Наименование оператора связи и (или) провайдера хостинга	ПАО МЕГАФОН
3.	Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель)	Контроль за технологическим, производственным оборудованием
4.	Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), протоколов взаимодействия	Проводной
Сведения о программных и программно-аппаратных средствах, используемых на объекте критической информационной инфраструктуры		
1.	Наименования программно-аппаратных средств (пользовательских компьютеров, серверов, телекоммуникационного оборудования, средств беспроводного доступа, иных средств) и их количество	- DELL T630 16SFF 2xE5-2603v3 32GB (1 шт.) - Intel Core i7 13700KF (3шт.) - Dahua DH-PFS4420-16GT-240 (1 шт.)
	Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии)	Astra Linux 1.7 (Сервера, АРМ) RouterOS v. 7.13.1 SwitchOS v. 2.13
	Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем)	Прикладное ПО резервного копирования RuBackup Прикладное ПО 1С: Предприятие Прикладное ПО 1С: Документооборот Прикладное ПО 1С: Зарплата и Бухгалтерия
4.	Применяемые средства защиты информации (в том числе встроенные в общесистемное, прикладное программное обеспечение) (наименования средств защиты информации, реквизиты сертификатов соответствия, иных документов, содержащих результаты оценки соответствия средств защиты информации или сведения о непроведении такой оценки) или сведения об отсутствии средств защиты информации	Встроенные общесистемные прикладные средства, сертификация и экспертиза средств информации не производилась.
Иные сведения		

1.	Сведения о наличии средств архивирования и резервного копирования данных	Отсутствуют
	Сведения о подключении ЗОКИИ к корпоративному (ведомственному) центру ГосСОПКА	С центрами ГосСОПКА не взаимодействует
3.	Сведения об установленных на ЗОКИИ средствах ГосСОПКА	Средства ГосСОПКА отсутствуют

Таблица 1. Технические характеристики и состав ЗОКИИ

ФГБУ НПП ГАММА

№ п/п	Наименование элемента значимого объекта КИИ	Сетевое имя	Провайдер	Доменное имя	Внешний IPадрес	Внутренний IP-адрес	Используемые протоколы	ОС	ППО	Название учетных записей	Лицо, ответственное за эксплуатацию	Лицо, ответственное за администрирование	Средства защиты
1.	Маршрутизатор MikroTik RB5009UPr+S+IN	route_dmz	ПАО «МЕГАФОН	–	192.168.2.1	10.1.0.1	tcp, udp, snmp, ssh	RouterOS 7	-	adm_dmz	Системный администратор	Системный администратор	Межсетевой экран Рубикон
	Маршрутизатор MikroTik RB5009UPr+S+IN	route_local	–	–	–	10.2.0.1	tcp, udp, snmp, ssh	RouterOS 7	-	adm_local	Системный администратор	Системный администратор	Встроенные в общесистемное ПО алгоритмы и средства. Межсетевой экран Рубикон.
	Коммутатор Mikrotik CRS328-24P-4S+RM	switch	–	–	–	–	–	SwitchOS	–	admin	Старший системный администратор	Старший системный администратор	Встроенные в общесистемное ПО алгоритмы и средства.
	Сервер DEPO Storm 1430T4R на базе Intel Xeon W-3345 3.4 GHz	srv1	–	proxy.univer	–	10.1.11.2	tcp, udp, ssh, http, https	Astra Linux 1.7	-	admin	Администратор	Администратор	Встроенные в общесистемное ПО алгоритмы и средства. Межсетевой экран Рубикон. САВЗ – Kaspersky Endpoint Security for Linux

№ п/п	Наименование элемента значимого объекта КИИ	Сетевое имя	Провайдер	Доменное имя	Внешний IPадрес	Внутренний IP-адрес	Используемые протоколы	ОС	ППО	Название учетных записей	Лицо, ответственное за эксплуатацию	Лицо, ответственное за администрирование	Средства защиты
	Сервер DEPO Storm 1430T4R на базе Intel Xeon W-3345 3.4 GHz	srv2	–	dc.univer	–	10.0.2.3	tcp, udp, ssh,	Astra Linux 1.7	Active Directory	admin	Администратор	Администратор	Встроенные в общесистемное ПО алгоритмы и средства. Межсетевой экран Рубикон. САВЗ – Kaspersky Endpoint Security for Linux

Таблица 2 - Состав значимого объекта КИИ ФГБУ НПП «ГАММА»

Раздел 2. События (условия), при наступлении которых начинается реализация предусмотренных Планом мероприятий

- Предупреждения от систем обнаружения вторжений (IDS/IPS).
- Обнаружение потенциальных угроз безопасности;
- Выявление вторжений в сеть и выявление аномальной активности на сетевых устройствах;
- Сбор сведений с использованием информационно- коммуникационных технологий:
    1. сканирование информационного ресурса;
    2. прослушивание (захват) сетевого трафика;
    3. социальная инженерия.
- Зарегистрированные попытки несанкционированного доступа;
- Изменения в системных ресурсах;
- Превышение нормативов использования процессора, памяти или сети;
- Выявление системные ошибок, приводящие к сбоям в работе;
- Осуществление своевременных обновлений и внедрение критических исправлений;
- Необходимость внедрения критических исправлений для предотвращения известных уязвимостей;
- Мошенничество с использованием информационно- коммуникационных технологий:
    1. злоупотребление при использовании информационного ресурса;
    2. публикация мошеннического информационного ресурса.

2.1 Источники информации о КИ на ЗОКИИ

СЗИ:

– Оповещения центра управления антивирусного ПО, поступающие на узел Администратора ИБ;

– Отказы в доступе внутрисистемных компонентов межсетевого экранирования (брандмауэра конечной точки и межсетевого экрана на границе сети);

– Оповещения, создаваемые в результате работы подсистемы защиты информации от несанкционированного доступа;

– Оповещения, создаваемые системой мониторинга сетевых ресурсов ЛВС Университет ИБ, аудит отказов и нагрузки элементов ЛВС;

Журналы, полученные в результате агрегации всех отчетов средств защиты информации Университет ИБ;

- Отчеты о результатах выполнения резервного копирования данных элементов ЗОКИИ и их состояния;
- Системы анализа и детектирования уязвимостей внутренней сетевой инфраструктуры.

Пользовательские, административные и внешние источники информации:

– Сотрудники учреждения, ответственные за ИБ: Администратор ИБ, Старший системный администратор, Руководитель ИБ, Системный администратор;

– Уведомления или информирование ДИТ;

– Уведомления или информирование ФСТЭК России или НКЦКИ о наличии угроз ИБ.

Раздел 3. Мероприятия, проводимые в ходе реагирования на компьютерные инциденты и принятия мер по ликвидации последствий

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
1. Обнаружение и регистрация КИ								
1.	Доклад Старшему системному администратору	Устный доклад	Старший системный администратор	Администратор ИБ	Ч + 5 мин.			
2.	Заполнение карточки КИ	Карточка КИ (форма в электронном виде)	Старший системный администратор	Администратор ИБ	Ч + 10 мин.	После выполнения п. 1.1.	В карточку внесена запись о КИ	
3.	Заполнение журнала КИ	Журнал в электронном виде	Старший системный администратор	Администратор ИБ	Ч + 15 мин.	После выполнения п. 1.2.	Журнал КИ заполнен	
4.	Информирование ответственного лица, уполномоченного предоставлять сведения о КИ в ДИТ, НКЦКИ	Устный доклад	Администратор ИБ	Руководитель ИБ	Ч + 10 мин.	После выполнения п. 1.3.		
5.	Информирование руководителя Университета о КИ	Устный доклад	Руководитель ИБ	Руководитель организации	Ч + 15 мин.	После выполнения п. 1.4.		
2. Определение вовлеченных в КИ элементов информационной инфраструктуры								
1.	Сбор сообщений от технических средств	Общесистемное ПО, САВЗ	Администратор ИБ	Руководитель ИБ	Ч + 25 мин.	После выполнения п. 1.5.		
2.	Сбор сообщений от работников, пользователей, привилегированных пользователей	Опрос / получение письменных объяснений	Администратор ИБ	Руководитель ИБ	Ч + 30 мин.	После выполнения п. 2.1.		
3.	Сбор доказательств	Журналы регистрации событий, копий жестких дисков и других данных, собранных на предшествующих этапах и т.п.	Администратор ИБ	Руководитель ИБ	Ч + 35 мин.	После выполнения п. 2.2.		
4.	Сбор сведений об уязвимостях, посредством которых были реализованы угрозы ИБ	Сканер уязвимостей	Администратор ИБ	Руководитель ИБ	Ч + 30 мин.	После выполнения п. 2.1.		

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
5.	Сбор данных, зафиксированных системами контроля доступа и видеонаблюдения		Администратор ИБ	Руководитель ИБ	Ч + 40 мин.	После выполнения п. 2.4.		
3. Определение очередности реагирования на КИ								
1.	Определение очередности реагирования на КИ, исходя из оценки уровня влияния КИ и приоритета	Сбор информации по последствиям КИ, определение уровня влияния и приоритетов	Администратор ИБ	Руководитель ИБ	Ч + 50 мин.	После выполнения п. 2.5.		
4. Локализация КИ								
1.	Направление ответственного за ИБ для проведения диагностических работ по выявлению и локализации КИ	Флеш-накопитель, дистрибутивы СЗИ, образы ПО	Администратор ИБ	Руководитель ИБ	Ч + 60 мин.	После выполнения 2.5.		
2.	Отключение пораженных элементов ЗОКИИ	-	Администратор ИБ	Руководитель ИБ	Ч + 60 мин.	После выполнения 4.1.		
3.	Блокировка скомпрометированных учетных записей	АРМ, Серверное оборудование (Контроллер домена)	Администратор ИБ	Руководитель ИБ	Ч + 1 ч. 05 мин.	После выполнения 4.2.		
4.	Изъятие съемных носителей	Жесткий диск, флеш-накопитель	Администратор ИБ	Руководитель ИБ	Ч + 60 мин.	После выполнения 4.3.		
5.	Визуальный осмотр мест размещения ЗОКИИ на предмет выявления и фиксации попыток несанкционированной установки ПО, установки внешних носителей информации, нарушения опломбирования, нарушения целостности кабельной инфраструктуры и иных нарушений информационной безопасности ЗОКИИ/ОКИИ и его компонентов	Журналы СЗИ	Администратор ИБ	Руководитель ИБ	Ч + 1 ч. 20 мин.	После выполнения 4.4.		
6.	Мониторинг и фиксация попыток	Журналы СЗИ	Администратор ИБ	Руководитель ИБ	Ч + 1 ч. 50 мин.	После выполнения 4.5.		

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
	несанкционированной установки ПО, установки внешних носителей информации и иных действий, проводимых на оборудовании, АРМ и серверах, входящих в периметр ЗОКИИ/ОКИИ.							
7.	Передача данных о проведенных работах по локализации КИ	Устный доклад или телефон или электронная почта	Администратор ИБ	Руководитель ИБ	Ч + 2 ч. 30 мин.	После выполнения 4.6.		
8.	Протоколирование действий по локализации	АРМ	Диспетчер ИБ	Руководитель ИБ	Ч + 2 часа 40 мин.	После выполнения 4.7.		
5.	**Информирование курирующего ОИВ, ДИТ, НКЦКИ и внешних организаций**							
1.	Уведомление курирующего ОИВ о КИ	Телефон или электронная почта	Руководитель ИБ	–	Ч + 30 мин.	После выполнения 1.6.		
2.	Уведомление ДИТ о КИ	Электронная почта: dit_incident@mos.ru	Руководитель ИБ	–	Ч + 40 мин.	После выполнения 5.1.		
3.	Информирование внешних организаций о компрометации ключей электронной подписи	Электронная почта, телефон	Руководитель ИБ	–	Ч + 50 мин.	После выполнения 5.2.		
4.	Уведомление НКЦКИ о КИ	Электронная почта: incident@cert.gov.ru или по телефону: +7 (916) 901-07-42.	Руководитель ИБ	–	Ч + 60 мин.	После выполнения 5.3.		
5.	Доведение сведений о проведенных мероприятиях по информированию до руководителя ИБ	Личный доклад	Руководитель ИБ	–	Ч + 3 ч.	После выполнения п. 5.4.		
6.	**Выявление последствий КИ**							
1.	Выявление работоспособности СВТ		Администратор ИБ	Руководитель ИБ	Ч + 3 ч. 30 мин.	После выполнения п. 4.7.		
2.	Протоколирование выявленных последствий	АРМ	Администратор ИБ	Руководитель ИБ	Ч + 4 ч.	После выполнения п. 6.1.	Внесение данных в протокол	
7.	**Ликвидация последствий КИ**							
1.	Использование всех возможных мер по восстановлению работоспособности ЗОКИИ	АРМ, загрузка антивируса, обновление ПО и смена скомпрометирован ных паролей, восстановление	Администратор ИБ	Руководитель ИБ	Ч + 4 ч. 30 мин.	После выполнения п. 6.1.		

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
		данных из резервных копий, удаление вредоносного кода, восстановление настройки технических средств, связанности элементов ЗОКИИ, Проведение нагрузочного тестирования т.д						
2.	Протоколирование действий по ликвидации последствий КИ	АРМ	Администратор ИБ	Руководитель ИБ	Ч + 4 ч. 45 мин.	После выполнения п. 7.1.		
3.	Доклад о произведенных работах по ликвидации последствий КИ ответственным лицам	Личный доклад	Администратор ИБ	Руководитель ИБ	Ч + 5 ч.	После выполнения п. 7.2.		
8. Привлечение ФСБ России к ликвидации последствий КИ								
1.	Решение о привлечении ФСБ России, если работоспособность ЗОКИИ не восстановлена	Устное решение	Руководитель ИБ	–	Ч + 6 ч.	После выполнения п. 7.3.	Устное решение	
2.	Внесение в журнал отметки об информировании НКЦКИ о необходимости привлечения должностных лиц ФСБ России	Журнал, ручка	Руководитель ИБ	–	Ч + 6 ч. 10 мин.	После выполнения п. 8.1.		
3.	Направление в НКЦКИ дополнительных материалов	АРМ, Электронная почта: incident@cert.gov.ru	Руководитель ИБ	–	Ч + 6 ч. 30 мин.	После выполнения п. 8.2.		
4.	Получение от НКЦКИ подтверждения о привлечении ФСБ России	Электронная почта, телефон	Руководитель ИБ	–	Ч + 8 ч.	После выполнения п. 8.3.		
5.	Организация взаимодействия с подразделениями и должностными лицами ФСБ России	Пропуск к ЗОКИИ, АРМ	Руководитель ИБ	–	Ч + 10 ч.	После выполнения п. 8.4.		
9. Закрытие КИ								
1.	Издание приказа о проведении расследования	Приказ, согласованный и подписанный в установленном порядке	Руководитель ИБ		Ч + 30 ч.	После выполнения п. 8.5.		

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
2.	Проведение расследования КИ, выявление причин возникновения и оценивание нанесённого ущерба КИ ЗОКИИ	Просмотр и обработка логфайлов АРМ, записей видеокамер внутреннего наблюдения, данных СКУД и других имеющихся технических и административных возможностей учреждения, не противоречащих действующему законодательств, изучение объяснительных, служебных записок от персонала	Администратор ИБ	Руководитель ИБ	Ч + 30 ч. 30 мин.	После выполнения п. 9.1.	Проект акта по результатам проведённого расследования КИ, причины возникновения, условия и обстоятельства КИ	
3.	Информирование руководителя ИБ о проведенном расследовании	Устный доклад	Администратор ИБ	Руководитель ИБ	Ч + 35 ч. 30 мин.	После выполнения п. 9.2.		
4.	Подписание акта по результатам проведённого расследования КИ	Оформленный акт	Руководитель ИБ	–	Ч + 36 ч.	После выполнения п. 9.3.	Подписанный акт	
5.	Информирование ДИТ, ОИВ о результатах расследования КИ и о нанесенном ущербе КИ	Электронная почта: dit_incident@mos.ru	Руководитель ИБ	–	Ч + 36 ч. 20 мин.	После выполнения п. 9.4.		
6.	Информирование ЦОДД о закрытии КИ	Электронная почта, телефон	Руководитель ИБ	–	Ч + 36 ч. 50 мин.	После выполнения п. 9.5.		
7.	Направление в НКЦКИ результатов расследования КИ	Электронная почта: incident@cert.gov.ru или по телефону: +7 (916) 901-07-42	Руководитель ИБ	–	Ч + 48 ч.	После выполнения п. 9.6.		
8.	Внесение журнал КИ о времени оповещения НКЦКИ о результатах расследования КИ	АРМ	Руководитель ИБ	–	Ч + 48 ч. 30 мин.	После выполнения п. 9.7.		
10. Анализ результатов деятельности по управлению КИ								
1.	Разработка рекомендаций по устранению в информационных ресурсах	Рекомендации по принятию дополнительных мер	Руководитель ИБ, Администратор	Руководитель ИБ	Ч + 7 дней	После выполнения п. 9.8.	Рекомендации доложены руководителю	

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
	причин и условий возникновения КИ	защиты информации в соответствии с нормативными правовыми актами и методическими документами уполномоченных федеральных органов исполнительной власти (ФСБ России и ФСТЭК России), в том числе доработку (актуализацию) и/или разработку документации, регламентирующей вопросы обеспечения безопасности организации; рекомендации по повышению защищенности информационных ресурсов от компьютерных атак; рекомендации по устранению технических причин и условий, способствующих проведению деструктивного воздействия на информационные ресурсы.	ИБ, Старший системный администратор					
2.	Оценка результатов и эффективности реагирования на КИ, предусмотренная Планом	Оценка достаточности и эффективности процессов и процедур реагирования на компьютерные инциденты, изложенных в Плане; предложения по включению в План дополнительных	Руководитель ИБ, Администратор ИБ, Старший системный администратор	Руководитель ИБ	Ч + 10 дней	После выполнения п. 10.1.	Рабочее совещание проведено	

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
		процессов и процедур, которые могли бы повысить эффективность действий, выполняемых на стадиях «обнаружение и регистрация КИ» и «реагирование на КИ»; предложения по использованию дополнительных инструментальных средств с целью повышения эффективности реагирования и установления причин и условий возникновения КИ; оценка эффективности обмена информацией о КИ между всеми сторонами, принимающими участие на стадиях «обнаружение и регистрация КИ» и «реагирование на КИ»						
3.	Внесение изменений в План реагирования на КИ и принятия мер по ликвидации последствий КА и его утверждение	АРМ, План	Руководитель ИБ	–	Ч + 14 дней	После выполнения п. 10.2.		При необходимости и по решению руководства
4.	Отправка проекта Плана реагирования на КИ и принятия мер по ликвидации последствий КА на согласование в ФСБ России	Проект Плана, письмо в ФСБ	Руководитель ИБ	–	Ч + 16 дней	После выполнения п. 10.3.		Если в Плане задействованы силы ФСБ России
5.	Доработка проекта Плана реагирования на КИ и принятия мер по ликвидации последствий	Проект Плана, письмо в ФСБ	Руководитель ИБ	–	Ч + 20 дней	После выполнения п. 10.4.		Если требуется внести изменения по

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
	КА с учетом мнения ФСБ России							результатам согласования
6.	Утверждение Плана реагирования на КИ и принятия мер по ликвидации последствий КА	План	Руководитель ИБ	–	Ч + 25 дней	После выполнения п. 10.5.		
7.	Направление копии измененного Плана реагирования на КИ и принятия мер по ликвидации последствий КА в НКЦКИ	Копия утвержденного Плана	Руководитель ИБ	–	Ч + 32 дня	После выполнения п. 10.6		

Раздел 4. Подразделения и должностные лица, ответственные за проведение мероприятий по реагированию на КИ и принятие мер по ликвидации последствий КА

№ п/п	Ответственноелицо (ФИО) / должность	Роль	Контактные данные	Адрес электронной почты	Адрес и место размещения (номер кабинета)	Реквизиты приказа (распоряжения)
1.	**Иванов Иван Иванович, Руководитель организации**	Возлагает на заместителя руководителя организации полномочия по ИБ Создает подразделение по ИБ Принимает решение о привлечении подразделений и должностных лиц ФСБ России к проведению мероприятий по реагированию на КИ	Телефон: 8 800 555 35 35	ivanov@npp.gamma.ru	Профсоюзная ул., 78, стр. 4	Приказ (распоряжение)от 09.01.2024 № 23/ДР ДСП
2.	**Смирнов Петр Иванович Заместитель генерального директора**	Курирует деятельность по обеспечению ИБ; Взаимодействует с ФСБ России, ФСТЭК России, ГосСОПКА (НКЦКИ), РКН, СМИ, ОИВ, внешними и отраслевыми регуляторами, ДИТ, поставщиками услуг (подрядчиками), лицензиатами, субъектами КИИ при проведении мероприятий по реагированию на КИ; Информирует руководство о КИ; Руководит структурным подразделением по ИБ; Координирует работу и действия Участников процесса. Осуществляет выработку рекомендаций/проведение мероприятий по недопущении КИ на	Телефон: 8 925 517 266 87	smirnov@npp.gamma.ru	Профсоюзная ул., 78, стр. 4	Приказ (распоряжение)от 09.01.2024 № 24/ДР ДСП

		ЗОКИИ в будущем.				
3	**Корнеев Иван Филиппович, Администратор ИБ**	Передаёт поступившую информацию в НКЦКИ, ДИТ, курирующий ОИВ, ЦОДД; Получает сообщения, рекомендации и предписания от НКЦКИ; Проводит предварительную проверку состояния ИБ ЗОКИИ; Участвует в мероприятиях по реагированию КИ ЗОКИИ; Передаёт данные о КИ (пункт №4 Карточки КИ), на бумажном носителе или посредством служебной электронной почты Администратору ИБ; Передаёт информацию о произошедшем КИ руководителю ИБ; Выполняет полученные рекомендации и предписания от НКЦКИ; Проводит расследование КИ ЗОКИИ;	Телефон: 8 977 395 98 89	korneev@npp.gamma.ru	Профсоюзная ул., 78, стр. 4	Приказ (распоряжение)от 09.01.2024 № 25/ДР

4	**Агафонов Евгений Олегович, старший диспетчер поддержки**	Принимает от диспетчера поддержки информацию об инциденте информационной безопасности на объекте контроля и управления (ЗОКИИ). Осуществляет регистрацию инцидента в общем Журнале инцидентов. Передает полученные данные в Национальный киберцентр по компьютерной безопасности и координирующие структуры, такие как Департамент информационных технологий, ответственный за объекты информационно-вычислительной инфраструктуры, и Центр обработки данных и диспетчеризации. Получает сообщения, рекомендации и предписания от НКЦКИ и передает полученную информацию обратно в Журнал учёта инцидентов. Ведет протоколирование совершенных действий.	Телефон: 8 906 078 98 78	agafonov@npp.gamma.ru	Профсоюзная ул., 78, стр. 4	Приказ (распоряжение)от 09.01.2024 № 26/ДР
5	**Сидоров Илья Петрович, Системный администратор**	Эксплуатирует и администрирует ЗОКИИ; Участвует в мероприятиях по выявлению, реагированию и расследованию КИ ЗОКИИ.	Телефон: 8 495 528 31 17	sidorov@npp.gamma.ru	Профсоюзная ул., 78, стр. 4	Приказ (распоряжение) от 09.01.2024 № 27/ДР

Раздел 5. Условия привлечения подразделений и должностных лиц ФСБ России

Условиями привлечения подразделений и должностных лиц ФСБ России к проведению мероприятий по реагированию на КИ и принятию мер по ликвидации последствий компьютерных атак являются следующие:

– Инцидент привёл к прекращению функционирования ЗОКИИ;

– Инцидент привел к возникновению неблагоприятных последствий в социальной, экономической, политической, экологической и оборонной сфере;

– Выполненные должностными лицами субъекта КИИ мероприятия не позволили ликвидировать последствия КИ, связанного с функционированием ЗОКИИ (восстановить штатное функционирование ЗОКИИ).

Раздел 6. Порядок проведения мероприятий по реагированию на КИ и принятию мер по ликвидации последствий КА в отношении ЗОКИИ совместно с привлекаемыми подразделениями и должностными лицами ФСБ России

Доклад руководителя ИБ (Смирнов Петр Иванович) о необходимости привлечения подразделений и (или) должностных лиц ФСБ России к проведению мероприятий по реагированию на КИИ и принятию мер по ликвидации последствий КА. Решение руководителя организации о необходимости привлечения подразделений и должностных лиц ФСБ России. В течение 30 минут:

Внесение в карточку КИ отметки о привлечении должностных лиц ФСБ России к реагированию на КИ и ликвидации последствий КА. Подготовка и направление в НКЦКИ дополнительных материалов (Смирнов Петр Иванович).

Получение от НКЦКИ подтверждения о привлечении ФСБ России.

Заместитель генерального директора организует взаимодействие с подразделениями и должностными лицами ФСБ России с целью ликвидации последствий КА.