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: Загороднов Е.А.

Проверил:
Р. В. Пимонов

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.

21. Приказ ФСБ России от 19.06.2019 года№281 "Об утверждении Порядка, технических условий установки и эксплуатации средств ГосСОПКА".

22. Федеральный закон от 27.06.2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации".

23. Федеральный закон от 26.07.2017 года № 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".

Согласно приведенным разделам необходимо создать План реагирования на компьютерные инциденты для ИСПДН БАНКА ПАО ЗЕНИТБАНК.

План реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак

Раздел 1. Технические характеристики и состав ЗОКИИ

Сведения о взаимодействии объекта критической информационнойинфраструктуры 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 взаимодействияобъекта критической информационной инфраструктуры с сетями электросвязи	Отсутствует взаимодействие ЗОКИИ с сетью связи общего пользования, а также наложенными или выделенными сетями. Объект расположен локально в пределахинженерного сооружения.
2.	Наименование оператора связи и (или) провайдера хостинга	Информация отсутствует
3.	Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель)	Информация отсутствует
4.	Способ взаимодействия с сетью электросвязи с указанием типа доступа к сети электросвязи (проводной, беспроводной), протоколов взаимодействия	Проводной/Беспроводной
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	- СА-7200, DIU-N4, СА-ШУЗ, - АРМ 11th Gen Intel(R) Core(TM) I7-13500KF, 3.75 GHz, 1.52 GHz (32 АРМ)

2.	Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии)	- Linux, CentOS, Windows 10, AstaLinux
3.	Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключениемприкладных программ, входящих в состав дистрибутивов операционных систем)	- FIRE 1
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	- Бэкап-Сервер
2.	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

1.1. Состав значимого объекта КИИ «АИСПДН БАНКА ПАО ЗЕНИТБАНК»

№	Наименование элемента значимого объекта КИИ	Сетевое имя	Провайдер	Доменное имя	Внешний IP-адрес	Внутренний IP-адрес	Используемые протоколы	ОС[5]	ППО[6]	Название учетных записей	Лицо, ответственное за эксплуатацию[7]	Лицо, ответственное за администрирование	Средства защиты
1.	Сервер №1	server	ISP A	-	203.0.113.10	192.168.1.10	TCP/IP, SSH, HTTP	Linux CentOS 8	Apache, OpenSSH	admin, user1, user2	Кузьмин Алексей	Иванов Петр	Firewall, IDS
2.	Сервер №2 для Бэкапа	backup	ISP D	backup.local	198.51.100.20	192.168.2.15	TCP/IP, SSH, FTP	Ubuntu 20.04 LTS	Bacula, OpenSSH	backup_admin,	Колькин Игорь	Белорусов Иван	Backup software, Firewall
2.	АРМ сотрудника организации №1	ARM1	-	-	198.51.100.5	192.168.0.25	TCP/IP, SMB	Windows 10	Microsoft Office, Мой офис	Пользвотлель 1	Магомед Шуман	Прусикин Демид	Внутренний VPN компании
3.	АРМ сотрудника организации №2	ARM2	-	-	198.51.100.5	192.168.0.25	TCP/IP, SMB	Windows 10	Microsoft Office, Мой офис	Пользователь 2	Кузьмина Ирига	Иванова Елена	Внутренний VPN компании
4.	АРМ сотрудника организации №3	ARM3	-	-	198.51.100.5	192.168.0.25	TCP/IP, SMB	Astra Linux	Microsoft Office, Мой офис	Пользователь 3	Сидорова Евгений	Куров Петр	Внутренний VPN компании

5.	Маршрутизатор	marshtis	-	-	192.0.2.1	192.168.0.1	TCP/IP, ICMP	Cisco	-	adminMarsh	Минин Михаил	Желобанов Александр	ACLs, VPN
6.	Бэкап-сервер	Backup server	-	-	198.51.100.20	192.168.2.15	TCP/IP, SSH, FTP	Ubuntu 20.04 LTS	Bacula, OpenSSH	backup_admin, backup_user	Жулин Петр	Петров Дмитрий	Backup software, Firewall
7.	Шлюз безопасности	security	-	-	203.0.113.50	192.168.3.1	TCP/IP, VPN	pfSense	-	adminShlus	Яковлев Иван	Сидоров Кирилл	IDS, Firewall, Proxy

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;

Регистрация попыток несанкционированного доступа;

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;

Замедление, временный сбой или прекращение работы АРМ, сервисов и иных компонентов ЗОКИИ;

Нарушение установленного в организации режима доступа к информации или компонентам ЗОКИИ;

Функционирование ВПО;

Несанкционированное изменение информации на элементах ЗОКИИ;

Превышение допустимой нагрузки на вычислительные ресурсы элементов ЗОКИИ;

Отказ функционирующего на элементах ЗОКИИ программного и аппаратного обеспечения;

Иные нарушения в работе элементов ЗОКИИ, вызывающих прекращение выполнения его целевых функций.

2.1 Источники информации о КИ на ЗОКИИ

СЗИ:

Оповещения антивирусного ПО и внутрисистемных компонентов межсетевого экранирования (брандмауэр);

Данные журналов событий ПО, операционных систем серверов и автоматизированных рабочих мест, систем резервного копирования и других систем;

Оповещения средств автоматического или автоматизированного мониторинга информационной безопасности учреждения;

Оповещения и уведомления СЗИ.

Пользовательские, административные и внешние источники информации:

Сотрудники учреждения, ответственные за ИБ: Главный администратор управления ИБ, заместитель главного администратора управлений ИБ, Руководитель ИБ по участку №1, старший диспетчер поддержки, диспетчер поддержи, начальник дежурной смены, пользователи;

Уведомления или информирование ДИТ;

Уведомления или информирование ФСТЭК России или НКЦКИ о наличииугроз ИБ;

СМИ.

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								
1.1.	Немедленное уведомление начальнику дежурной смены о возникшем инциденте, о КИ	Устный доклад	Диспетчер поддержи	Начальник дежурной смены	Ч + 5 мин.		Доклад озвучен	
1.2.	Заполнение карточки КИ	Карточка, распечатанная на бумаге, ручка / АРМ (форма в электронной форме)	Диспетчер поддержи	Начальник дежурной смены	Ч + 10 мин.	После выполнения п. 1.1	В карточку внесена запись о КИ	
1.3.	Заполнение журнала КИ	Оформленный по форме журнал, ручка/электронный вид	Старший диспетчер поддержки	Начальник дежурной смены	Ч + 15 мин.	После выполнения п. 1.2	В журнал внесена запись о КИ	
1.4.	Немедленное информирование ответственного лица, уполномоченного предоставлять сведения о КИ в ДИТ, НКЦКИ о произошедшем КИ (старшего диспетчера)	Устный доклад	Начальник дежурной смены	Ответственное лицо, уполномоченное предоставлять сведения о КИ в ДИТ, НКЦКИ о произошедшем КИ	Ч + 10 мин.	После выполнения п. 1.3	Информация передана ответственному лицу	
1.5.	Незамедлительное информирование ответственного за ИБ участка о КИ	Устный доклад	Начальник дежурной смены	Руководитель ИБ по участку№1	Ч + 15 мин.	После выполнения п. 1.4	Информация передана ответственному ИБ участка	

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
	администратора о произошедшем КИ							
1.6.	Немедленное информирование заместителя руководителя ИБ участка о произошедшем КИ	Устный доклад	Руководитель ИБ по участку№1	Заместитель главного адм. управления ИБ	Ч + 20 мин.	После выполнения п. 1.5	Информация передана заместителю главного адм. управления ИБ	
1.7.	Незамедлительное информирование главного администратора управления ИБ о произошедшем КИ	Устный доклад	Заместитель главного адм. управления ИБ	Главный администратор управления ИБ	Ч + 25 мин.	После выполнения п. 1.6	Информация передана главному администратору управления ИБ	
1.8.	Направление дежурной бригады на место размещения ЗОКИИ для выяснения обстоятельств, приведших к ошибке/сбою	Служебный транспорт, необходимый инструмент (отвертки, гаечные ключи и т.д.), дистрибутивы СЗИ, запасное имущество и принадлежности (ЗИП)	Начальник дежурной смены	Заместитель главного администратора отдела ИБ	Ч + 25 мин.	После выполнения п. 1.7	Выполнено отправление на место размещения ЗОКИИ	Служебный транспорт
2. Определение вовлеченных в КИ элементов информационной инфраструктуры								
2.1.	Сбор сообщений от технических средств	Общесистемное ПО	Руководитель ИБ по участку№1	Заместитель главного адм. управления ИБ	Ч + 25 мин.	После выполнения п. 1.6	Сообщения собраны	
2.2.	Сбор сообщений от работников, пользователей,	Опрос / получение письменных объяснений	Заместитель главного адм. управления ИБ	Главный администратор управления ИБ	Ч + 30 мин.	После выполнения п. 1.7	Сообщения собраны	

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
	привилегированных пользователей							
2.3.	Сбор доказательств	Журналы регистрации событий, копий жестких дисков и других данных, собранных на предшествующих этапах и т.п.	Заместитель главного адм. управления ИБ	Главный администратор управления ИБ	Ч + 35 мин.	После выполнения п 2.2	Доказательства собраны	
2.4.	Сбор сведений об уязвимостях, посредством которых были реализованы угрозы ИБ	Сканер уязвимостей	Руководитель ИБ по участку№1	Заместитель главного адм. управления ИБ	Ч + 30 мин.	После выполнения п 2.1	Собраны сведения об уязвимостях	
2.5.	Сбор данных, зафиксированных системами контроля доступа и видеонаблюдения		Руководитель ИБ по участку№1	Заместитель главного адм. управления ИБ	Ч + 40 мин.	После выполнения п 2.4	Собраны сданные о системах контроля доступа и видеонаблюд	
3. Определение очередности реагирования на КИ								
3.1.	Определение очередности реагирования на КИ, исходя из оценки уровня влияния КИ и приоритета	Сбор информации по последствиям КИ, определение уровня влияния и приоритетов (по масштабу и по значимости)	Заместитель главного адм. управления ИБ	Главный администратор управления ИБ	Ч + 50 мин.	После выполнения п 2.3	Определена очередность реагирования на КИ	

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
			4.	**Локализация КИ**				
4.1.	Направление ответственного за ИБ для проведения диагностических работ по выявлению и локализации КИ	Служебный транспорт, флеш-накопитель, дистрибутивы СЗИ, образы ПО и т.д.	Руководитель ИБ по участку№1	Заместитель главного адм. управления ИБ	Ч + 60 мин.	После выполнения п 2.5	Направлен ответственны для проведения диагностики	
4.2.	Отключение пораженных элементов ЗОКИИ	-	Руководитель ИБ по участку№1	Заместитель главного адм. управления ИБ	Ч + 60 мин.	После выполнения п 4.1	Отключены пораженные элементы ЗОКИИ	
4.3.	Блокировка скомпрометированных учетных записей	АРМ пользователя	Руководитель ИБ по участку№1	Заместитель главного адм. управления ИБ	Ч + 1 ч. 05 мин.	После выполнения п 4.2	Заблокированы скомпрометированные УЗ	
4.4.	Изъятие съемных носителей	Жесткий диск, флеш-накопитель	Заместитель главного адм. управления ИБ	Главный администратор управления ИБ	Ч + 60 мин.	После выполнения п 3.1	Изъяты съемные носители	
4.5.	Визуальный осмотр мест размещения ЗОКИИ на предмет выявления и фиксации попыток несанкционированной установки ПО, установки внешних носителей информации, нарушения опломбирования, нарушения	ПАК СЗИ для выявления КИ	Руководитель ИБ по участку№1	Заместитель главного адм. управления ИБ	Ч + 1 ч. 20 мин.	После выполнения п 4.3	Осмотр визизуальный, где размещены ЗОКИИ, выполнен	

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
	целостности кабельной инфраструктуры и иных нарушений информационной безопасности ЗОКИИ/ОКИИ и его компонентов							
4.6.	Мониторинг и фиксация попыток несанкционированной установки ПО, установки внешних носителей информации и иных действий, проводимых на оборудовании, АРМ и серверах, входящих в периметр ЗОКИИ/ОКИИ.	ПАК СЗИ для выявления КИ	Руководитель ИБ по участку№1	Заместитель главного адм. управления ИБ	Ч + 1 ч. 50 мин.	После выполнения п 4.5	Осуществлен мониторинг и фиксация попыток несанкционированной установки ПО	
4.7.	Передача данных о проведенных работах по локализации КИ, диспетчеру старшему для дальнейшего информирования заместителя главного адм. управления ИБ	Устный доклад/ телефон/ электронная почта	Руководитель ИБ по участку№1	Заместитель главного адм. управления ИБ	Ч + 2 ч. 30 мин.	После выполнения п 4.6	Осуществлена передача данных о проведенных работах по локализации	

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
4.8.	Протоколирование действий по локализации	АРМ	старший диспетчер поддержки	Руководитель ИБ по участку№1	Ч + 2 часа 40 мин.	После выполнения п 4.7	Осуществлено протоколирование действий по локализации	
5. Информирование курирующего ОИВ, ДИТ, НКЦКИ, поставщиков услуг (подрядчиков) и внешних организаций								
5.1.	Уведомление курирующего ОИВ о КИ	Телефон/ электронная почта	старший диспетчер поддержки	Руководитель ИБ по участку№1	Ч + 30 мин.	После выполнения п. 1.7	Уведомление передано с помощью телефона и продублировано на корпоративную почту	
5.2.	Уведомление ДИТ о КИ (посредством электронной почты:)	Электронная почта: **ibpomzh @zenit.ru**	старший диспетчер поддержки	Руководитель ИБ по участку№1	Ч + 40 мин.	После выполнения п. 5.1	Уведомление передано по корпоративной почте	
5.3.	Информирование внешних организаций о компрометации ключей электронной подписи	Электронная почта, телефон	старший диспетчер поддержки	Руководитель ИБ по участку№1	Ч + 50 мин.	После выполнения п. 5.2	Осуществлено информирование внешних организаций	
5.4.	Уведомление поставщиков услуг (подрядчиков)	Телефон/ электронная почта	старший диспетчер поддержки	Руководитель ИБ по участку№1	Ч + 60 мин.	После выполнения п. 5.3	Уведомление передано поставщикам услуг	
5.5.	Уведомление НКЦКИ о КИ	Электронная почта: **ibpomzh @zenit.ru** или позвоните по телефону: +7 (953) 555-55-55.	старший диспетчер поддержки	Руководитель ИБ по участку№1	Ч + 3 ч.	После выполнения п. 4.9	Уведомление передано НКЦКИ	

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
5.6.	Доведение сведений о проведенных мероприятиях по информированию старшим диспетчер поддержкии руководителю ИБ участка	Личный доклад	старший диспетчер поддержки	Руководитель ИБ по участку№1	Ч + 3 ч. 10 мин.	После выполнения п. 5.6	Осуществлена передача сведений о проведённые мероприятиях по информированию	
6. Выявление последствий КИ								
6.1.	Выявление работоспособности СВТ		Руководитель ИБ по участку№1	Заместитель главного адм. управления ИБ	Ч + 3 ч. 30 мин.	После выполнения п. 4.7	Выявлена работоспособность	
6.2.	Протоколирование выявленных последствий	АРМ	старший диспетчер поддержк и	Руководитель ИБ по участку№1	Ч + 4 ч.	После выполнения п. 6.1	Оформлен протокол выявленных последствий	
7. Ликвидация последствий КИ								
7.1.	Использование всех возможных мер по восстановлению работоспособности ЗОКИИ	АРМ, загрузка антивируса, обновление ПО и смена скомпрометированных паролей, восстановление данных из резервных копий, удаление вредоносного кода, восстановление настройки технических средств,	Руководитель ИБ по участку№1	Заместитель главного адм. управления ИБ	Ч + 4 ч. 30 мин.	После выполнения п. 6.1	Осуществление всех мер по восстановлению работоспособности ЗОКИИ	

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
		связанности элементов ЗОКИИ, Проведение нагрузочного тестирования т.д.						
7.2.	Протоколирование действий по ликвидации последствий КИ	АРМ	Старший диспетчер поддержки	Руководитель ИБ по участку№1	Ч + 4 ч. 45 мин.	После выполнения п. 7.1	Оформлен протокол действий по ликвидации КИ	
7.3.	Доклад о произведенных работах по ликвидации последствий КИ старшего диспетчера поддержки для Руководителя ИБ по участку№1	Личный доклад	Старший диспетчер поддержки	Руководитель ИБ по участку№1	Ч + 5 ч.	После выполнения п. 7.2	Доклад озвучен	
8. Привлечение ФСБ России к ликвидации последствий КИ								
8.1.	Решение о привлечении ФСБ России, если работоспособность ЗОКИИ не восстановлена	Устное решение	Главный администратор управления ИБ		Ч + 6 ч.	После выполнения п. 7.3	Принято решение	
8.2.	Внесение в журнал отметки об информировании НКЦКИ о	Журнал, ручка	Старший диспетчер поддержки	Руководитель ИБ по участку№1	Ч + 6 ч. 10 мин.	После выполнения п. 8.1	Поставлена отметка в журнал	

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
	необходимости привлечения должностных лиц ФСБ России							
8.3.	Направление в НКЦКИ дополнительных материалов	АРМ, Электронная почта: **ibpomzh @zenit.ru**	Старший диспетчер поддержки	Руководитель ИБ по участку№1	Ч + 6 ч. 30 мин.	После выполнения п. 8.2	Переданы дополнительные материалы	
8.4.	Получение от НКЦКИ подтверждения о привлечении ФСБ России	Электронная почта, телефон	Старший диспетчер поддержки	Руководитель ИБ по участку№1	Ч + 8 ч.	После выполнения п. 8.3	Получено потверждение о НКЦКИ	
8.5.	Организация взаимодействия с подразделениями и должностными лицами ФСБ России	Пропуск к ЗОКИИ, АРМ	Руководитель ИБ по участку№1	Заместитель главного адм. управления ИБ	Ч + 10 ч.	После выполнения п. 8.4	Организовано взаимодействие с подразделениями должностными лицами ФСБ Россииии	
9. Закрытие КИ								
9.1.	Издание приказа о проведении расследования	Приказ, согласованный и подписанный в	Заместитель главного адм. управления ИБ	Главный администратор управления ИБ	Ч + 30 ч.	После выполнения п. 8.5	Приказ создан и издан	

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
		установленном порядке		организации по вопросам ИБ				
9.2.	Проведение расследования КИ, выявление причин возникновения и оценивание нанесённого ущерба КИ ЗОКИИ	Просмотр и обработка лог-файлов АРМ, записей видеокамер внутреннего наблюдения, данных СКУД и других имеющихся технических и административных возможностей учреждения, не противоречащих действующему законодательству, изучение объяснительных, служебных записок от персонала	Руководитель ИБ по участку№1	Заместитель главного адм. управления ИБ	Ч + 30 ч. 30 мин.	После выполнения п. 9.1	Проведено расследование КИ и создан АКТ по результатам проведенного расследования	
9.3.	Информирование Заместителя главного адм. управления ИБ о проведенном расследовании	Устный доклад	Руководитель ИБ по участку№1	Заместитель главного адм. управления ИБ	Ч + 35 ч. 30 мин.	После выполнения п. 9.2	Информация передана	
9.4.	Подписание акта по результатам проведенного расследования КИ	Оформленный акт	Руководитель ИБ по участку№1	Заместитель главного адм. управления ИБ	Ч + 36 ч.	После выполнения п. 9.3	Подписан акт	

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
9.5.	Информирование ДИТ, ОИВ о результатах расследования КИ и о нанесенном ущербе КИ	Электронная почта: **ibpomzh @zenit.ru**	Старший диспетчер поддержки	Руководитель ИБ по участку№1	Ч + 36 ч. 20 мин.	После выполнения п. 9.4	Информация передана ДИТ и ОИВ	
9.6.	Информирование ЦОДД о закрытии КИ	Электронная почта, телефон	Старший диспетчер поддержки	Руководитель ИБ по участку№1	Ч + 36 ч. 50 мин.	После выполнения п. 9.5	Информация передана ЦОДД	
9.7.	Направление в НКЦКИ результатов расследования КИ	Электронная почта: incident@cert.gov.ru или позвоните по телефону: +7 (916) 901-07-42.	Старший диспетчер поддержки	Руководитель ИБ по участку№1	Ч + 48 ч.	После выполнения п. 9.6	Информация передана	
9.8.	Внесение журнал КИ о времени оповещения НКЦКИ о результатах расследования КИ	Журнал, ручка / АРМ	Старший диспетчер поддержки	Руководитель ИБ по участку№1	Ч + 48 ч. 30 мин.	После выполнения п. 9.7	Информация внесена в журнал	
10. Анализ результатов деятельности по управлению КИ]								
10.1.	Разработка рекомендаций по устранению в информационных ресурсах причин и условий возникновения КИ	Рекомендации по принятию дополнительных мер защиты информации в соответствии с нормативными правовыми актами	Заместитель главного адм. управления ИБ , , Руководитель ИБ по участку№1, Старший диспетчер поддержки, диспетчер поддержки начальник дежурной смены	Главный администратор управления ИБ	Ч + 7 дней	После выполнения п. 9.8	Рекомендации составлены	

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
		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						

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
		воздействия на информационные ресурсы.						
10.2.	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 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	Заместитель главного адм. управления ИБ , , Руководитель ИБ по участку№1, Старший диспетчер поддержки, диспетчер поддержки начальник дежурной смены	Главный администратор управления ИБ	Ч + 10 дней	После выполнения п. 10.1	Осуществлена оценка результатов и эффективности и реагирования на КИ	

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
		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».						
10.3.	Внесение изменений в План реагирования на КИ и принятия мер по ликвидации последствий КА и его утверждение	АРМ, План	Заместитель главного адм. управления ИБ	Главный администратор управления ИБ	Ч + 14 дней	После выполнения п. 10.2	Осуществлено внесение изменений в план реагирования	При необходимости
10.4.	Отправка проекта Плана реагирования на КИ и принятия мер по ликвидации последствий КА на согласование в ФСБ России	Проект Плана, письмо в ФСБ	Заместитель главного адм. управления ИБ	Главный администратор управления ИБ	Ч + 16 дней	После выполнения п. 10.3	Отправлен проект плана реагирования на КИ	При задействовании сил ФСБ

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
10.5.	Доработка проекта Плана реагирования на КИ и принятия мер по ликвидации последствий КА с учетом мнения ФСБ России	Проект Плана, письмо в ФСБ	Заместитель главного адм. управления ИБ	Главный администратор управления ИБ	Ч + 20 дней	После выполнения п. 10.4	Осуществлена доработка проекта плана реагирования на КИ и приняты меры по ликвидации последствий КА	При необходимости внести изменения
10.6.	Утверждение Плана реагирования на КИ и принятия мер по ликвидации последствий КА	План	Заместитель главного адм. управления ИБ	Главный администратор управления ИБ	Ч + 25 дней	После выполнения п. 10.5	Утвержден план	
10.7.	Направление копии измененного Плана реагирования на КИ и принятия мер по ликвидации последствий КА в НКЦКИ	Копия утвержденного Плана	Заместитель главного адм. управления ИБ	Главный администратор управления ИБ	Ч + 32 дня	После выполнения п. 10.6	Отправлена копия плана с добавленными пунктами	

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.	**Кудряшов Евгений Дмитриевич, Руководитель организации**	Делегирует заместителю руководителя организации ответственность за обеспечение информационной безопасности. Формирует структурное подразделение по вопросам информационной безопасности. Принимает решение о привлечении подразделений и должностных лиц ФСБ России для проведения мероприятий по реагированию на инциденты информационной безопасности.	Телефон: 88001567855	kudr@zenit.ru		Приказ (распоряжение)от 25.12.2023 № 555
2.	**Шаляпин Игорь Васильевич, Главный администратор управления ИБ**	Курирует мероприятия по обеспечению информационной безопасности и взаимодействует с рядом организаций, включая ФСБ России, ФСТЭК России, ГосСОПКА (НКЦКИ), РКН, СМИ, органы внутренних дел (ОИВ), внешних и отраслевых регуляторов, Департамент информационных технологий (ДИТ), поставщиков услуг (подрядчиков), лицензиатов и субъектов контроля и управления информационной безопасностью (КИИ) в ходе реагирования на инциденты информационной	Телефон: 896745612432	shalyp@zenit.ru		Приказ (распоряжение) От 25.12.2023 №555

		безопасности. Регулярно информирует руководство об инцидентах. Осуществляет руководство структурным подразделением по информационной безопасности и получает от начальника этого подразделения информацию о произошедших инцидентах на объекте контроля и управления (ЗОКИИ/ОКИИ).				
3	**Петрухин Иван Григорьевич, Заместитель главного администратора управления ИБ**	Получает от лица, ответственного за информационную безопасность, информацию о инциденте на объекте контроля и управления (ЗОКИИ). Передает полученные данные главному администратору управления ИБ организации по вопросам информационной безопасности. Совместно с руководителем ИБ по участку №1 проводит расследование случившегося инцидента на ЗОКИИ. Координирует действия всех участников процесса и разрабатывает рекомендации или осуществляет мероприятия для предотвращения подобных инцидентов в будущем.	Телефон: 89153457895	petryxin@zenit.ru		Приказ (распоряжение) от 25.12.2023 № 555

4	**Быков Владислав Олегович, Руководитель ИБ по участку №1**	Осуществляет предварительную проверку состояния информационной безопасности объекта контроля и управления (ЗОКИИ) и активно участвует в мероприятиях по реагированию на инциденты информационной безопасности на ЗОКИИ. Передает информацию о случившихся инцидентах (согласно пункту №4 Карточки инцидента) старшему поддержки пользователя на бумажном носителе или через служебную электронную почту. Кроме того, передает данные о произошедшем инциденте дежурной смене и заместителю главного администратора ИБ. Соблюдает рекомендации и предписания от Национального киберцентра по компьютерной безопасности (НКЦКИ), проводит расследование инцидента на ЗОКИИ и сообщает заместителю главного администратора управления ИБ и старшему диспетчеру поддержки о результатах проведенного расследования.	Телефон: 89997899090	Bykov@zenit.ru		Приказ (распоряжение) от 25.12.2023 № 555

5.	**Дымов Андрей Сергеевич, начальник дежурной смены**	Осуществляет общий контроль и руководство действиями дежурной смены в период ее дежурства. В случае утраты автоматизированного управления и мониторинга параметров объекта контроля и управления (ЗОКИИ/ОКИИ), направляет дежурную бригаду для активации управления в режиме "ручного/местного".	Телефон: 89673215434	dymov@zenit.ru		Приказ (распоряжение) от 25.12.2023 № 555
6	**Ларионов 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: 89541234323	larionov@zenit.ru		Приказ (распоряжение) от 25.12.2023 № 555

7	**Петров Евгений Дмитриевич, Диспетчер поддержки**	Регистрирует недоступность для автоматизированного управления, контроля и мониторинга параметров ЗОКИИ в результате сбоя или неисправности в ее функционировании. Сообщает о случившемся руководителю дежурной смены, заполняет форму инцидента (карточку КИ) и направляет ее Старшему диспетчеру поддержки. Осуществляет регистрацию инцидента в Журнале учёта КИ и получает уведомления и инструкции от старшего диспетчера поддержки НКЦКИ.	Телефон: 8775670990	pertove@zenit.ru		Приказ (распоряжение) от 25.12.2023 № 555

Раздел 5. Условия привлечения подразделений и должностных лиц ФСБ России

Условиями для вовлечения подразделений и должностных лиц ФСБ России в проведение мероприятий по реагированию на компьютерные инциденты (КИ) и принятию мер по устранению их последствий являются следующие:

1) Произошедший инцидент привел к полной остановке функционирования объекта контроля и управления информацией (ЗОКИИ).

2) Предпринятые должностными лицами, ответственными за информационную безопасность субъекта контроля и управления информацией (КИИ), меры не привели к успешному восстановлению нормальной работы ЗОКИИ.

3) Национальному киберцентру по компьютерной безопасности (НКЦКИ) направлено уведомление о КИ, связанном с функционированием ЗОКИИ, с указанием необходимости привлечения подразделений и должностных лиц ФСБ России, а также о причинах, по которым предпринятые должностными лицами субъекта КИИ меры не устранили последствия инцидента.

В каждом случае для ЗОКИИ/НОКИИ могут быть установлены иные условия, при которых осуществляется привлечение подразделений и должностных лиц ФСБ России.

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

Главный администратор управления информационной безопасности (И.В. Шаляпин) представляет руководству организации (Е.Д. Кудряшову) доклад о неотложной необходимости вовлечения подразделений и (или) должностных лиц ФСБ России для выполнения мероприятий по реагированию на компьютерные инциденты и устранению их последствий. Решение об этом принимается руководителем организации. В течение 30 минут:

1) Вносится отметка в карточку инцидента о привлечении должностных лиц ФСБ России для реагирования на инцидент и ликвидации его последствий (И.Г. Петрухин, Заместитель главного администратора управления информационной безопасности).

2) Подготавливаются и направляются в Национальный киберцентр по компьютерной безопасности (НКЦКИ) дополнительные материалы (И.Г. Петрухин, Заместитель главного администратора управления информационной безопасности).

3) Получается подтверждение от НКЦКИ о привлечении ФСБ России.

4) Главный администратор управления информационной безопасности организует сотрудничество с подразделениями и должностными лицами ФСБ России.