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 №8

по дисциплине: «Управление информационной безопасностью»

Выполнила:
Студентка группы ББМО-02-22
Бардасова И.А.

Проверил:
Пимонов Р.В.

Москва, 2024

Содержание

Перечень сокращений

В настоящем документе используются сокращения, они приведены в таблице 1.

Таблица 1 – Перечень сокращений

Сокращение	Обозначение
АСУ ТП	Автоматизированная система управления технологическим процессом
ВПО	Вредоносное программное обеспечение
ГосСОПКА	Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации
ДИТ	Департамент информационных технологий города Москвы
ЗОКИИ	Значимый объект критической информационной инфраструктуры
ИБ	Информационная безопасность
КА	Компьютерная атака
КИ	Компьютерный инцидент
КИИ	Критическая информационная инфраструктура Российской Федерации
КоАП РФ	Кодекс Российской Федерации об административных правонарушениях
Минпромторг России	Министерство промышленности и торговли Российской Федерации
Минцифры России	Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации
Минтранс России	Министерство транспорта Российской Федерации
Минэнерго России	Министерство энергетики Российской Федерации
НКЦКИ	Национальный координационный центр по компьютерным инцидентам
НОКИИ	Незначимый объект критической информационной инфраструктуры Российской Федерации
ОИВ	Орган исполнительной власти города Москвы
Орган (организация)	Органы исполнительной власти города Москвы, подведомственные им государственные учреждения города Москвы, находящиеся в их ведомственном подчинении государственных унитарных предприятий города Москвы
ПАК	Программно-аппаратный комплекс

Сокращение	Обозначение
План	План реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак на значимые объекты критической информационной инфраструктуры Российской Федерации
Роскомнадзор	Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций
РФ	Российская Федерация

Нормативные ссылки

Настоящие Методические рекомендации разработаны с учетом требований законодательства Российской Федерации:

1. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ;
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
3. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
4. Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;
5. Постановление Правительства Российской Федерации от 17.02.2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
6. Постановление Правительства Российской Федерации от 15.07.2022 № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)»;
7. Приказ ФСБ России от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на

информационные ресурсы Российской Федерации»;

8. Приказ ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения»;

9. Приказ ФСБ России от 06.05.2019 № 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»;

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

11. Приказ ФСБ России от 13.02.2023 № 77 «Об утверждении Порядка взаимодействия операторов с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, включая информирование ФСБ России о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных»;

12. Приказ ФСБ России от 11.05.2023 № 213 «Об утверждении порядка осуществления мониторинга защищенности информационных

ресурсов, принадлежащих федеральным органам исполнительной власти, высшим исполнительным органам государственной власти субъектов Российской Федерации, государственным фондам, государственным корпорациям (компаниям), иным организациям, созданным на основании федеральных законов, стратегическим предприятиям, стратегическим акционерным обществам и системообразующим организациям российской экономики, юридическим лицам, являющимся субъектами критической информационной инфраструктуры Российской Федерации либо используемых ими»;

13. Приказ Роскомнадзора от 14.11.2022 № 187 «Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных»;

14. Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;

15. Приказ ФСТЭК России от 22.12.2017 № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»;

16. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

17. Постановление Правительства Москвы от 23.12.2021 № 2170-ПП «Об утверждении Положения о координации деятельности органов исполнительной власти города Москвы и подведомственных им организаций в области обеспечения безопасности информации, обрабатываемой с использованием средств автоматизации, в том числе в информационно-

телекоммуникационных сетях»;

18. Распоряжение Департамента информационных технологий города Москвы от 12.09.2022 № 64-16-434/22 «Об утверждении порядка предоставления сведений об инцидентах информационной безопасности»;

19. Рекомендации ФСТЭК России по повышению уровня безопасности информационных ресурсов при установлении в Российской Федерации уровней опасности проведения целевых компьютерных атак;

20. Методические рекомендации НКЦКИ по разработке Плана реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации;

21. Методические рекомендации НКЦКИ по установлению причин и ликвидации последствий компьютерных инцидентов, связанных с функционированием информационных ресурсов российской федерации;

22. Инструкция НКЦКИ по формированию электронного письма уведомления о компьютерном инциденте, атаке или уязвимости.

23. Методические рекомендации по установлению причин и ликвидации последствий компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации;

24. ГОСТ Р 59709-2022 «Защита информации. Управление компьютерными инцидентами. Термины и определения» утвержден приказом Росстандарта от 29 ноября 2022 года № 1375-ст;

25. ГОСТ Р 59710-2022 «Защита информации. Управление компьютерными инцидентами. Общие положения» утвержден приказом Росстандарта от 29 ноября 2022 года № 1376-ст;

26. ГОСТ Р 59711-2022 «Защита информации. Управление компьютерными инцидентами. Организация деятельности по управлению компьютерными инцидентами» утвержден приказом Росстандарта от 29 ноября 2022 года № 1377-ст;

27. ГОСТ Р 59712-2022 «Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты» утвержден приказом Росстандарта от 29 ноября 2022 года № 1378-ст.

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

Раздел 1. Технические характеристики и состав ЗОКИИ ООО «СТРОЙСТРИТ»

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.	Внутренняя ЛВС, присоединённая к сети связи общего пользования
2.	Наименование оператора связи и (или) провайдера хостинга.	Телекоммуникационная компания ПАО «Ростелеком»
3.	Цель взаимодействия с сетью электросвязи (передача (прием) информации, оказание услуг, управление, контроль за технологическим, производственным оборудованием (исполнительными устройствами), иная цель).	Взаимодействие с целью оказания услуг
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.	**Серверы:** Сервер Dell PowerEdge T40 1xE-2224G 1x8GbUD x3 1x1Tb 7.2K 3.5" SATA RW 1G 1P 1x290W 1Y NBD Cabled – 1 шт. **Компьютеры:** TREIDCOMPUTERS – 2 шт. **Телекоммуникационное оборудование и средства беспроводного доступа:** Коммутатор ZYXEL GS1200-8 (Управляемый L2, 8 портов) – 2 шт. Маршрутизатор MMIKROTIK RB2011ILS-IN – 1 шт.

		Источник бесперебойного питания: CROWN CMU-SP2000IEC USB CM000003132 – 2 шт.
2.	Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии).	**Операционные системы и платформы:** Microsoft Windows Server Standard 2019, включает в себя Active Directory и BitLocker. Windows 11 **Системы мониторинга и управления:** Zabbix **Сертификат безопасности, создающий зашифрованное соединение между веб-сервером и веб-браузером:** SSL означает Secure Sockets Layer **Программа для резервного копирования данных:** Veeam Backup & Replication
3.	Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем).	SAP ERP for Oil and Gas Energy Trading and Risk Management (ETRM) System
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.	Антивирусное ПО ESET SERVER SECURITY, Антивирусное ПО Dr.Web, Лицензия СКЗИ «КриптоПро CSP» версии 5.0 на одном рабочем месте, ПАК: SafeNet Network Logon 8 сертификат ФСТЭК № 2792, Kaspersky Endpoint Security, Active Directory и BitLocker
Иные сведения		

1.	Сведения о наличии средств архивирования и резервного копирования данных.	Сервер резервного копирования: настроим резервирование БД каждые 15 минут
2.	Сведения о подключении ЗОКИИ к корпоративному (ведомственному) центру ГосСОПКА.	С центрами ГосСОПКА не взаимодействует
3.	Сведения об установленных на ЗОКИИ средствах ГосСОПКА.	Отсутствуют

Состав КИИ ООО «СТРОЙСТРИТ»

№ п/ п	Наименование элемента значимого объекта КИИ	Сетевое имя	Провай-дер	Доменное имя	Внешний IP-адрес	Внут-ренний IP-адрес	Использу-емые протоко-лы	ОС	ППО	Название учетных записей	Лицо, ответственное за эксплуатацию	Лицо, ответственное за администриро-вание	Средства защиты
1.	Сервер	server-stroystrit	Ростелеком	-	195.131.40.150	11.0.0.1	tcp, udp, ssh, http, https, smtp	Microsoft Windows Server Standard 2019	MS SQL Server, SAP ERP for Oil and Gas, Active Directory, Zabbix	server	Власов Тимофей Владимирович	Крупко Дмитрий Олегович	Антивирусное ПО ESET SERVER SECURITY, Kaspersky Endpoint Security, Active Directory и BitLocker
2.	Коммутатор ZYXEL GS1200-8	zyxel	Ростелеком	-	-	11.0.0.2	tcp, udp, ssh, http, https	-	-	admin	Фиников Владислав Дмитриевич	Фиников Владислав Дмитриевич	Встроенные
3.	Маршрутизатор MMIKROTIK RB2011ILS-IN	m-router	-	-	-	11.0.0.3	tcp, udp, snmp, ssh	-	-	admin	Фиников Владислав Дмитриевич	Крупко Дмитрий Олегович	-
4.	АРМ 1	User1	-	-	-	11.0.0.4	tcp, udp, ssh	Windows 11	MS Office, Zabbix	adminu1	Цветкова Валерия Михайловна	Фиников Владислав Дмитриевич	Антивирусное ПО Dr.Web, Лицензия СКЗИ «КриптоПро CSP» версии 5.0 на одном рабочем месте, ПАК: SafeNet Network

													Logon 8 сертификат ФСТЭК № 2792
5.	АРМ 2	User2	-	-	-	11.0.0.5	tcp, udp, ssh	Windows 11	MS Office, Zabbix	adminu2	Шинко Илья Григорьевич	Фиников Владислав Дмитриевич	Антивирусное ПО Dr.Web, Лицензия СКЗИ «КриптоПро CSP» версии 5.0 на одном рабочем месте, ПАК: SafeNet Network Logon 8 сертификат ФСТЭК № 2792

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

1. Несанкционированное изменение информации на элементах ЗОКИИ;

2. Замедление, временный сбой или прекращение работы АРМ, сервера и иных компонентов ЗОКИИ;

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

4. Превышение допустимой нагрузки на вычислительные ресурсы элементов ЗОКИИ;

5. Отказ функционирующего на элементах ЗОКИИ программного и аппаратного обеспечения;

6. Ошибки в результате загрузки и применении обновлений ПО ЗОКИИ;

7. Предупреждения от систем обнаружения вторжений ЗОКИИ.

Источники информации о КИ на ЗОКИИ

СЗИ:

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

2. Отказы в доступе внутрисистемных компонентов межсетевого экранирования как на узлах сети, так и на границах сети;

3. Оповещения, создаваемые системой мониторинга сетевых ресурсов, аудит отказов и нагрузки элементов ЛВС;

4. Оповещения, создаваемые в результате работы подсистемы защиты информации о несанкционированном доступе;

5. Журналы, полученные в результате агрегации всех отчетов средств защиты информации;

6. Отчеты о результатах выполнения резервного копирования данных элементов ЗОКИИ и их состояния;

Пользовательские, административные и внешние источники информации:

1. Сотрудники учреждения, ответственные за ИБ: Руководитель ИБ, Администратор ИБ, Системный администратор;

2. Уведомления или информирование ДИТ;

3. 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 компьютерных атак, а также время, отводимое на их реализацию

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
1. Обнаружение и регистрация КИ								
1.1.	Немедленное уведомление администратору ИБ, о КИ	Устный доклад	Системный администратор	Администратор ИБ	Ч + 5 мин.	Первым делом	Доклад озвучен и начинают предпринимать меры	
1.2.	Заполнение карточки КИ	Карточка, распечатанная на бумаге, ручка / АРМ (форма в электронной форме)	Системный администратор	Администратор ИБ	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	Системный администратор	Администратор ИБ	Ч + 15 мин.	После выполнения п. 1.2.	Журнал КИ заполнен	
1.4.	Информирование ответственного лица, уполномоченного предоставлять сведения о КИ в ДИТ, НКЦКИ	Устный доклад	Системный администратор	Руководитель ИБ	Ч + 10 мин.	После выполнения п. 1.3.	Информация передана ответственному лицу	
1.5.	Незамедлительное информирование руководителя ИБ о произошедшем КИ	Устный доклад	Системный администратор	Руководитель ИБ	Ч + 15 мин.	Одновременно с п. 1.4.	Информация передана руководителю ИБ	

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
2. Определение вовлеченных в КИ элементов информационной инфраструктуры								
2.1.	Сбор сообщений от технических средств	Общесистемное ПО, АВЗ	Администратор ИБ	Руководитель ИБ	Ч + 25 мин.	После выполнения п. 1.5.	Собрана информация	
2.2.	Сбор сообщений от пользователей, привилегированных пользователей	Опрос / получение письменных объяснений	Администратор ИБ	Руководитель ИБ	Ч + 30 мин.	После выполнения п. 2.1.	Информация передана руководителю ИБ	
2.3.	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.	Информация передана руководителю ИБ	
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.	Выполнено отправление на место размещения ЗОКИИ	
2.5.	Сбор данных, зафиксированных системами контроля доступа и видеонаблюдения		Администратор ИБ	Руководитель ИБ	Ч + 40 мин.	После выполнения п. 2.4.	Собраны сданные о системах контроля доступа и видеонаблюдения	
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 приоритета	Администратор ИБ	Руководитель ИБ	Ч + 50 мин.	После выполнения п. 2.3.	Определена очередность реагирования на КИ	
4. Локализация КИ								
4.1.	Направление ответственного за ИБ для проведения диагностических работ по выявлению и локализации КИ	Флеш-накопитель, дистрибутивы СЗИ, образы ПО и т.д.	Администратор ИБ	Руководитель ИБ	Ч + 60 мин.	После выполнения 2.5.	Решение для проведения диагностики	
4.2.	Отключение пораженных элементов ЗОКИИ	-	Администратор ИБ	Руководитель ИБ	Ч + 60 мин.	После выполнения 4.1.	Отключены пораженные элементы ЗОКИИ	

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
4.3.	Блокировка скомпрометированных учетных записей	АРМ, Серверное оборудование(Контроллер домена)	Администратор ИБ	Руководитель ИБ	Ч + 1 ч. 05 мин.	После выполнения 4.2.	Заблокированы скомпрометированные УЗ	
4.4.	Изъятие съемных носителей	Жесткий диск, флеш-накопитель	Администратор ИБ	Руководитель ИБ	Ч + 60 мин.	После выполнения 4.3.	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 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.	Визуальный осмотр зоны размещения ЗОКИИ	
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.	Журналы СЗИ	Администратор ИБ	Руководитель ИБ	Ч + 1 ч. 50 мин.	После выполнения 4.5.	Осуществлен мониторинг и фиксация попыток несанкционированной установки ПО	
4.7.	Передача данных о проведенных работах по локализации КИ	Электронная почта	Администратор ИБ	Руководитель ИБ	Ч + 2 ч. 30 мин.	После выполнения 4.6.	Осуществлена передача данных о проведенных работах по локализации	
4.8.	Протоколирование действий по локализации	АРМ	Администратор ИБ	Руководитель ИБ	Ч + 2 часа 40 мин.	После выполнения 4.7.	Осуществлено протоколирование действий по локализации	

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
5. Информирование курирующего ОИВ, ДИТ, НКЦКИ и внешних организаций								
5.1.	Уведомление курирующего ОИВ о КИ	Телефон или электронная почта	Руководитель ИБ	-	Ч + 30 мин.	После выполнения 1.7.	Уведомление передано с помощью телефона и продублировано на корпоративную почту	
5.2.	Уведомление ДИТ о КИ	Электронная почта: dit_incident@mos.ru	Руководитель ИБ	-	Ч + 40 мин.	После выполнения 5.1.	Уведомление передано по корпоративной почте	
5.3.	Информирование внешних организаций о компрометации ключей электронной подписи	Электронная почта, телефон	Руководитель ИБ		Ч + 50 мин.	После выполнения 5.2.	Осуществлено информирование внешних организаций	
5.4.	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.	Уведомление передано НКЦКИ	
5.5.	Доведение сведени проведенных мероприятиях информированию руководителя ИБ	Личный доклад	Руководитель ИБ	-	Ч + 3 ч.	После выполнения п. 5.4.	Уведомление руководителю ИБ	
6. Выявление последствий КИ								
6.1.	Выявление работоспособности СВТ		Администратор ИБ	Руководитель ИБ	Ч + 3 ч. 30 мин.	После выполнения п. 4.7.	Выявлена работоспособность	
6.2.	Протоколирование выявленных последствий	АРМ	Администратор ИБ	Руководитель ИБ	Ч + 4 ч.	После выполнения п. 6.1.	Внесение данных в протокол	
7. Ликвидация последствий КИ								
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, проведение нагрузочного тестирования и т.д.	Администратор ИБ	Руководитель ИБ	Ч + 4 ч. 30 мин.	После выполнения п. 6.1.	Выполнение мер по восстановлению работоспособности ЗОКИИ	

7.2.	Протоколирование действий по ликвидации последствий КИ	АРМ	Администратор ИБ	Руководитель ИБ	Ч + 4 ч. 45 мин.	После выполнения п. 7.1.	Оформлен протокол действий по ликвидации КИ	

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
7.3.	Доклад о произведенных работах по ликвидации последствий КИ ответственному лицу	Личный доклад	Администратор ИБ	Руководитель ИБ	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	Руководитель ИБ	-	Ч + 6 ч.	После выполнения п. 7.3.	Принято решение	
8.2.	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.	Внесена отметка в журнал	
8.3.	Направление в НКЦКИ дополнительных материалов	АРМ, Электронная почта: incident@cert.gov.ru	Руководитель ИБ	-	Ч + 6 ч. 30 мин.	После выполнения п. 8.2.	Переданы дополнительные материалы	
8.4.	Получение от НКЦКИ подтверждения о привлечении ФСБ России	Электронная почта, телефон	Руководитель ИБ	-	Ч + 8 ч.	После выполнения п. 8.3.	Получено подтверждение	
8.5.	Организация взаимодействия с подразделениями и должностными лицами ФСБ России	АРМ	Руководитель ИБ	-	Ч + 10 ч.	После выполнения п. 8.4.	Организовано взаимодействие с подразделениями и должностными лицами ФСБ России	
9. Закрытие КИ								
9.1.	Издание приказа о проведении расследования	Приказ, согласованный и подписанный в установленном порядке	Руководитель ИБ	-	Ч + 30 ч.	После выполнения п. 8.5.	Приказ создан и издан	

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 законодательств	Администратор ИБ	Руководитель ИБ	Ч + 30 ч. 30 мин.	После выполнения п. 9.1.	Проведено расследование КИ и создан АКТ по результатам проведенного расследования	

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
9.3.	Информирование руководителя ИБ о проведенном расследовании	Устный доклад	Администратор ИБ	Руководитель ИБ	Ч + 35 ч. 30 мин.	После выполнения п. 9.2.	Информация передана	
9.4.	Подписание акта по результатам проведённого расследования КИ	Оформленный акт	Руководитель ИБ	-	Ч + 36 ч.	После выполнения п. 9.3.	Подписанный акт	
9.5.	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.	Информация передана ДИТ и ОИВ	
9.6.	Информирование ЦОДД о закрытии КИ	Электронная почта, телефон	Руководитель ИБ	-	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 по телефону: +7 (916) 901-07-42	Руководитель ИБ	-	Ч + 48 ч.	После выполнения п. 9.6.	Информация передана	
9.8.	Внесение журнал КИ о времени оповещения НКЦКИ о результатах расследования КИ	АРМ	Руководитель ИБ	-	Ч + 48 ч. 30 мин.	После выполнения п. 9.7.	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 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.	Администратор ИБ, Системный администратор	Руководитель ИБ	Ч + 7 дней	После выполнения п. 9.8.	Рекомендации по устранению КИ доложены руководителю	
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 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»	Администратор ИБ, Системный администратор	Руководитель ИБ	Ч + 10 дней	После выполнения п. 10.1.	Осуществлена оценка	

№ п\п	Мероприятие	Средства реагирования	Силы реагирования	Куратор	Время выполнения	Последовательность	Результат	Примечание
10.3.	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.	Осуществлено внесение изменений в План реагирования	Строго по решению руководства
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	Руководитель ИБ	-	Ч + 16 дней	После выполнения п. 10.3.	Отправлен проект Плана реагирования на КИ	Только если в Плане задействованы силы ФСБ России
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	Руководитель ИБ	-	Ч + 20 дней	После выполнения п. 10.4.	Выполнена доработка проекта Плана	Если требуется внести изменения по результатам согласования
10.6.	Утверждение Плана реагирования на КИ и принятия мер по ликвидации последствий КА	План	Руководитель ИБ	-	Ч + 25 дней	После выполнения п. 10.5.	Утвержден план	
№ п\п	**Мероприятие**	**Средства реагирования**	**Силы реагирования**	**Куратор**	**Время выполнения**	**Последовательность**	**Результат**	**Примечание**
10.7.	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	Отправлена копия измененного Плана	

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

№ п/п	Ответственное лицо (ФИО) / должность	Роль	Контактные данные	Адрес электронной почты	Адрес и место размещения (номер кабинета)	Реквизиты приказа (распоряжения)
1.	Шишков Максим Александрович, 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	Тел. +7 111 222 33- 44	shishkov@list.ru	115035,г. Москва, ул. Ирина, д.104/2, к.3	Приказ (распоряжение) от 18.01.2024 №3
2.	Крупко Дмитрий Олегович, Руководитель ИБ	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 ЗОКИИ в будущем.	Тел. +7 111 222 33- 45	krupkod@list.ru	115035,г. Москва, ул. Ирина, д.104/2, к.3	Приказ (распоряжение) от 18.01.2024 №3
3.	Власов Тимофей Владимирович, 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; Эксплуатирует и администрирует ЗОКИИ; Участвует в мероприятиях по выявлению, реагированию и расследованию КИ ЗОКИИ.	Тел. +7 111 222 33- 46	VlasovKrutoi@list.ru	115035,г. Москва, ул. Ирина, д.104/2, к.3	Приказ (распоряжение) от 18.01.2024 №3
4.	Фиников Владислав Дмитриевич, Системный администратор	Регистрирует КИ в общем Журнале КИ; Вносит данные о КИ в журнал учёта КИ; Протоколирование действий; Фиксирует невозможность автоматизированного управления, контроля и мониторинга параметров ЗОКИИ, в результате сбоя/неисправности в работе ЗОКИИ; Заполняет карточку КИ.	Тел. +7 111 222 33- 47	finik@list.ru	115035,г. Москва, ул. Ирина, д.104/2, к.3	Приказ (распоряжение) от 18.01.2024 №3

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 КА являются следующие:

1. Инцидент привёл к прекращению функционирования ЗОКИИ;

2. Должностные лица субъекта КИИ не смогли ликвидировать последствия КИ;

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

Крупко Д.О., руководитель ИБ, предоставляет доклад Шишкову М.А., руководителю ООО «СТРОЙСТРИТ», о необходимости привлечения подразделений и (или) сотрудников ФСБ России к проведению мероприятий по реагированию на КИИ и принятию мер по ликвидации последствий КА.

Шишков М.А. принимает решение о необходимости вовлечения подразделений и персонала ФСБ России. В течение 30 минут должно быть произведено:

- Внесение в информационную карточку компьютерного инцидента отметки о привлечении сотрудников ФСБ России к реагированию и устранению последствий (Выполнил: Фиников В.Д., Системный администратор).

- Подготовка и направление в Национальный Компьютерный Центр Киберкомандования и Инцидентов (НКЦКИ) дополнительных материалов (Выполнил: Крупко Д.О., Руководитель ИБ).

- Получение подтверждения от НКЦКИ о привлечении ФСБ России.

- Крупко Д.О. организует взаимодействие с подразделениями и представителями ФСБ России с целью эффективного устранения последствий компьютерного инцидента.