МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«МИРЭА – Российский технологический университет»

Институт кибербезопасности и цифровых технологий

Практическая работа № 4.2

по дисциплине

«Управление информационной безопасностью»

Выполнил:

ББМО–01–22

Чадов В. Т.

Проверил:

Пимонов Р. В.

«Зачтено» «__»_____2023 г. _____

Москва 2023

Содержание

1. Перечень сокращений

В настоящем документе используются сокращения, приведенные 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 РоссийскойФедерации
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
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, подведомственныеим государственные учреждения города Москвы, находящиеся в их ведомственном подчинении государственных унитарных предприятий города Москвы
ПАК	Программно-аппаратный комплекс
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

2. 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.

3. Технические характеристики и состав ЗОКИИ

Таблица 2 – 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 «ВымпелКом»
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	- АРМ 13th Gen Intel Core I5-13600K, 3.5GHz (15 шт) - Cisco SFS 7000 Series InfiniBand

		- Cisco 2921/K9
2.	Наименование общесистемного программного обеспечения (клиентских, серверных операционных систем, средств виртуализации (при наличии)	Windows 10, Linux (Ubuntu)
3.	Наименования прикладных программ, обеспечивающих выполнение функций объекта по его назначению (за исключением прикладных программ, входящих в состав дистрибутивов операционных систем)	MS Office, Adobe reader, Yandex browser, MS SQL Server, Visual Studio Code
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
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

Таблица 3 – Состав значимого объекта КИИ «Цифровая Независимость»

№ п/п	Наименование элемента значимого объекта КИИ	Сетевое имя	Провайдер	Доменное имя	Внешний IPадрес	Внутренний IP-адрес	Используемые протоколы	ОС[1]	ППО[2]	Название учетных записей	Лицо, ответственное за эксплуатацию[3]	Лицо, ответственное за администрирование	Средства защиты
1.	Коммутатор Cisco SFS 7000 Series InfiniBand	comm	ПАО «ВымпелКом»	-	192.168.56.101	192.168.3.1	tcp, udp, ssh	Linux	-	admin	8	7	Встроенные общесистемные прикладные средства
2.	Роутер Cisco 2921/K9	router	-	-	-	192.168.3.2	tcp, udp, ssh	Linux	-	admin	8	7	Встроенные общесистемные прикладные средства
3.	АРМ	Arm1	-	-	-	192.168.3.10	tcp, udp, ssh	Windows 10	MS Office, Adobe reader, Yandex browser, MS SQL Server, Visual Studio Code	Arm 1	1	8	Встроенные общесистемные прикладные средства
4.	АРМ	Arm2	-	-	-	192.168.3.11	tcp, udp, ssh	Windows 10	MS Office, Adobe	Arm 2	2	8	Встроенные общесистемные

									reader, Yandex browser, MS SQL Server, Visual Studio Code				прикладные средства
5.	АРМ	Arm3	-	-	-	192.168.3.12	tcp, udp, ssh	Windows 10	MS Office, Adobe reader, Yandex browser, MS SQL Server, Visual Studio Code	Arm 3	3	8	Встроенные общесистемные прикладные средства

[1] Операционная система.

[2] Прикладное программное обеспечение.

[3] Указывается номер строки из Раздела 6 настоящего документа, в которой содержатся сведения о соответствующем должностном лице.

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

Список событий (условий), при наступлении которых начинается реализация защитных действий:

- Обнаружение угрозы безопасности локальной сети.
- Обнаружение вредоносного ПО или вирусов в системе.
- Обнаружение физической угрозы информационной системе.
- Сообщения от сотрудников о возможных проблемах или инцидентах безопасности.
- Несанкционированное изменение информации в информационной системе.
- Нарушение установленного в организации режима доступа к информации.
- Обнаружение аномального поведения пользователей в информационной системе.
- Иные нарушения в работе элементов ЗОКИИ, вызывающих прекращение выполнения его целевых функций.

Источники информации о КИ на ЗОКИИ среди СЗИ:

- Службы обнаружения вирусов и вредоносного программного обеспечения.
- Данные журналов событий ПО, операционных систем серверов и автоматизированных рабочих мест и других систем
- Системы безопасности периметра.
- Оповещения средств автоматического или автоматизированного мониторинга информационной безопасности учреждения.
- Оповещения и уведомления СЗИ ЗОКИИ/ОКИИ.

Пользовательские, административные и внешние источники информации:

- Сотрудники учреждения, ответственные за ИБ.
- Отчеты и жалобы пользователей и персонала компании о неправомерной активности и нарушениях правил безопасности.
- Уведомления или информирование ФСТЭК России, или НКЦКИ о наличии угроз ИБ.
- СМИ.

5. Мероприятия, проводимые в ходе реагирования на компьютерные инциденты и принятия мер по ликвидации последствий компьютерных атак, а также время, отводимое на их реализацию

Таблица 4 – Меры по ликвидации последствий от компьютерных атак

Наименование события (условия)	**Организационные/ технические меры**	**Ответственные лица**	**Время**
Обнаружение угрозы безопасности локальной сети	Предотвращение: Обучение персонала; Своевременное обновление всего ПО и включение автоматических обновлений безопасности; Проведение многофакторной аутентификации пользователей. Обнаружение: Мониторинг сетевых портов. Реагирование: Изоляция зараженных систем от остальных ресурсов; Пересоздание системы с целью предотвращения повторной атаки при помощи бэкдора.	Старший системный администратор	Обучение сотрудников: 3 месяца. Этап обнаружения: постоянные проверки. Время анализа и подготовки аналитической справки по инциденту: для рядового случая не более 60 минут; для критического инцидента не более 40 минут.
Обнаружение вредоносного ПО или вирусов в системе	Предотвращение: Обучение персонала; Ограниченный доступ к конфиденциальной информации. Обнаружение: Использование сертифицированного ПО для обнаружения вредоностного ПО; Мониторинг сетевых портов; Ведение журналов событий. Реагирование: Изоляция зараженных систем от остальных ресурсов; Оперативная ликвидация угрозы на зараженных системах.	Старший системный администратор, ИТ-администратор	Обучение сотрудников: 3 месяца. Этап обнаружения: постоянные проверки. Время анализа и подготовки аналитической справки по инциденту: для рядового случая не более 60 минут; для критического инцидента не более 40 минут.
Обнаружение физической угрозы информационной системе	Предотвращение: Обучение персонала; Внедрение охранной системы.	Глава охранной службы	Время: для критического инцидента не более 60 минут.

Сообщения от сотрудников о возможных проблемах или инцидентах безопасности.	Реагирование: Классификация поступившей информации, информирование ответственных лиц.	Руководители отделов	Бессрочно
Несанкционированное изменение информации в информационной системе.	Предотвращение: Обучение персонала; Ограниченный доступ к конфиденциальной информации; Выполнение всех требований законодательства по защите персональных данных.	Старший системный администратор, ИТ-администратор, Руководители отделов	Обучение сотрудников: 3 месяца. Остальные этапы – бессрочно
Нарушение установленного в организации режима доступа к информации.	Предотвращение: Обучение персонала; Ограниченный доступ к конфиденциальной информации; Проведение многофакторной аутентификации пользователей.	Старший системный администратор	Обучение сотрудников: 3 месяца. Остальные этапы – бессрочно. Время анализа и подготовки аналитической справки по инциденту: для рядового случая не более 60 минут; для критического инцидента не более 40 минут.
Обнаружение аномального поведения пользователей в информационной системе	Предотвращение: Обучение персонала; Выполнение всех требований законодательства по защите персональных данных. Обнаружение: Мониторинг сетевых портов; Ведение журналов событий. Реагирование: Оперативная ликвидация угрозы.	Руководители отделов, Старший системный администратор, ИТ-администратор	Обучение сотрудников: 3 месяца. Этап обнаружения: постоянные проверки. Время анализа и подготовки аналитической справки по инциденту: для рядового случая не более 60 минут; для критического инцидента не более 40 минут.

Иные нарушения в работе элементов ЗОКИИ, вызывающих прекращение выполнения его целевых функций.	Предотвращение: Обучение персонала. Реагирование: Оперативная ликвидация угрозы; Обращение в специальные службы.	Старший системный администратор, ИТ-администратор, Руководители отделов	Обучение сотрудников: 3 месяца. Этап обнаружения: постоянные проверки. Время анализа и подготовки аналитической справки по инциденту: для рядового случая не более 60 минут; для критического инцидента не более 40 минут.

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

Таблица 5 – Список ответственных за проведение мероприятий по реагированию на КИ и принятие мер по ликвидации последствий КА лиц

Ответственное лицо/ должность	**Роль**	**Контактные данные**
Корзун Никита Евгеньевич, генеральный директор	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	+7915 123 99 22 korzun@gmail.ru
Макаренков Сергей Александрович, заместитель руководителя организации по вопросам 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 Получает информацию о КИ на ЗОКИИ/ОКИИ от начальника структурного подразделения по ИБ	+7915 888 77 66 makarenkov@gmail.ru
Никуличев Михаил Юрьевич, куратор ИБ	Получает информацию о КИ на ЗОКИИ от ответственного за ИБ. Передаёт поступившую информацию заместитель руководителя организации по вопросам ИБ. Совместно с Ответственным за ИБ проводит расследование произошедшего КИ на ЗОКИИ. Координирует работу и действия Участников процесса. Осуществляет выработку рекомендаций/проведение мероприятий (совместно с Ответственным за ИБ) по недопущении КИ на ЗОКИИ в будущем.	+7915 000 11 22 nikulichev@gmail.ru

Теленгатор Ксения Эдуардовна, начальник дежурной смены	Осуществляет общее руководство и контроль за действиями дежурной смены во время её дежурства. При потере автоматизированного управления и мониторинга параметров ЗОКИИ/ОКИИ, направляет дежурную бригаду для включения управления в «ручном/местном».	+7915 333 22 11 telengator@gmail.ru
Иванов Станислав Валентинович, старший диспечер	Получает информацию от Диспетчера (оператора АСУ) о КИ на ЗОКИИ. Регистрирует КИ в общем Журнале КИ. Передаёт поступившую информацию в НКЦКИ, ДИТ, курирующий ОИВ, ЦОДД. Получает сообщения, рекомендации и предписания от НКЦКИ. Передаёт поступившую информацию от НКЦКИ Диспетчеру (оператору АСУ). Вносит данные о КИ в журнал учёта КИ. Протоколирование действий.	+7915 444 55 66 ivanovsv@gmail.ru
Лукин Андрей Сергеевич, ответственный за ИБ участка	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 Диспетчеру (оператору АСУ). Передаёт информацию о произошедшем КИ старшему дежурному смены и куратору ИБ. Выполняет полученные рекомендации и предписания от НКЦКИ. Проводит расследование КИ ЗОКИИ и информирует куратора ИБ и старшего диспетчера о результатах проведённого расследования	+7915 333 11 66 lukin@gmail.ru
Полковников Михаил Вадимович, администратор	Эксплуатирует и администрирует ЗОКИИ. Участвует в мероприятиях по выявлению, реагированию и расследованию КИ ЗОКИИ.	+7915 777 88 77 polkovnik@gmail.ru

7. 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. КИ привёл к прекращению функционирования ЗОКИИ. 2. Выполненные должностными лицами субъекта КИИ мероприятия не позволили ликвидировать последствия КИ, связанного с функционированием ЗОКИИ (восстановить штатное функционирование ЗОКИИ). 3. В НКЦКИ направлено сообщение о КИ, связанном с функционированием ЗОКИИ с указанием в нем необходимости привлечения подразделений и должностных лиц ФСБ России и причин, по которым выполненные должностными лицами субъекта КИИ мероприятия не позволили ликвидировать последствия КИ.

Для каждого ЗОКИИ/НОКИИ могут быть добавлены и другие условия, при которых могут привлекаться подразделения и должностные лица 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: КИ привёл к прекращению функционирования ЗОКИИ. Выполненные должностными лицами субъекта КИИ мероприятия не позволили ликвидировать последствия КИ, связанного с функционированием ЗОКИИ (восстановить штатное функционирование ЗОКИИ).

8. 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 заместителя руководителя организации по вопросам ИБ Макаренкова С.А. руководству организации Корзуну Н.Е. 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 (Полковников М.В., диспетчер). Готовит и направляет в НКЦКИ дополнительные материалы (Полковников М.В., диспетчер).

Получение от НКЦКИ подтверждения о привлечении ФСБ России.

Заместитель руководителя организации по вопросам ИБ организует взаимодействие с подразделениями и должностными лицами ФСБ России.