Министерство образования Саратовской области
государственное автономное профессиональное образовательное учреждение
Саратовской области «Балаковский политехнический техникум»

СОГЛАСОВАНО
Совет ГАПОУ СО «БПТ»
(протокол от 18.03.2026г. № 4)

УТВЕРЖДЕНО
приказом директора ГАПОУ СО «БПТ»
от «18» марта 2026 г. № 80

Подписан: Никулина Элла Александровна
DN: C=RU, S=Саратовская область, L=Балаково, T=Директор, O="ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ САРАТОВСКОЙ ОБЛАСТИ ""БАЛАКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ ТЕХНИКУМ""", СНИЛС=05641551451, ИНН=644106310058, E=balakovopolytech@mail.ru, G=Элла Александровна, SN=Никулина, CN=Никулина Элла Александровна
Основание: я подтверждаю этот документ своей удостоверяющей подписью
Местоположение: г.Балаково, Саратовской области
Дата: 2026-04-09 13:08:49

ВНУТРЕННИЙ СТАНДАРТ
по защите информации

СОГЛАСОВАНО
Юрисконсульт ГАПОУ СО «БПТ»
_____ Троценко О.А.
«18» марта 2026г.

Вступает в законную силу с 18 марта 2026 г. и действует до отмены или принятия нового стандарта

г. Балаково
2026г.

1. Общие положения:

1.1 Внутренний стандарт по защите информации (далее – Стандарт) разработан с целью обеспечения защиты информации от несанкционированного доступа, утечки, модификации и иных угроз путём установления единых требований к управлению доступом, конфигурации систем, защите устройств и мониторингу событий безопасности в соответствии с законодательством РФ и спецификой образовательной деятельности в ГАПОУ СО «Балаковский политехнический техникум» (далее – Учреждения).

Стандарт разработан на основании следующих нормативных правовых актов:

–Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

–Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

–Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;

–Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Основ государственной политики в сфере информационной безопасности Российской Федерации»;

–Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

–Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований по защите информации в информационных системах»;

–Приказ Минцифры России от 10.03.2022 № 186 «Об утверждении Требований к защите информации в государственных информационных системах»;

–ГОСТ Р 56939-2024 «Защита информации. Требования к функциональным свойствам средств защиты информации»;

–ГОСТ Р 59547-2021 «Защита информации. Мониторинг информационной безопасности. Общие положения».

1.2 Настоящий Стандарт является неотъемлемой частью организационных мер по обеспечению информационной безопасности на объектах информатизации Учреждения и входит в состав общих организационно-распорядительных мер, реализующихся в рамках Политики информационной безопасности Учреждения.

2. Область применения

2.1 Требования настоящего Стандарта распространяется на всех работников Учреждения, обучающихся, подрядчиков и/или иных лиц, имеющих доступ к информационным системам и содержащейся в них информации, включая персональные данные, образовательные ресурсы и служебную информацию.

2.2 Настоящий Стандарт (надо описать что еще применительно ко всем процессам, связанным с автоматизированной обработкой информации на объектах информатизации Учреждения)

3. Термины определения и сокращения

3.1 В настоящем Стандарте применены следующие термины с соответствующими определениями:

Автоматизированное рабочее место (далее – АРМ) – программно-технический комплекс автоматизированной (информационной) системы, предназначенный для автоматизации деятельности определенной категории пользователей или определенного вида деятельности.

Администратор информационной безопасности (далее – АИБ) – пользователь, уполномоченный выполнять действия по администрированию и/или управлению информационной системы и/или ее системы защиты информации в соответствии с установленной ролью.

Аутентификационная информация – информация, использующаяся при проверке подлинности субъекта или объекта доступа.

Аутентификация – действия по проверке подлинности субъекта и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации.

Доступ к информационной системе – использование информационных технологий и программно-технических средств обеспечивающих обработку сведений, находящихся в информационной системе и/или возможность ознакомления с такими сведениями.

Внешний пользователь – работник сторонней, по отношению к ГАПОУ СО «БПТ» организации и/или индивидуальный предприниматель, которому предоставляется доступ к информационным системам.

Внутренний пользователь – работник ГАПОУ СО «БПТ», которому предоставляется доступ к информационным системам.

Идентификатор доступа (далее – идентификатор) – признак субъекта или объекта доступа в виде строки знаков (символов), который используется при идентификации и однозначно определяет соотнесенную с ним идентификационную информацию.

Идентификационная информация – совокупность значений идентификационных атрибутов, которая связана с конкретным субъектом доступа или конкретным объектом доступа.

Информация ограниченного доступа – сведения, не предназначенные для общего и/или открытого использования, доступ к которой ограничен федеральными законами.

Информационная безопасность (далее – ИБ) – сохранение конфиденциальности, целостности и доступности информации.

Информационная система (далее – ИС) – система, состоящая из комплекса средств автоматизации, реализующего информационную технологию выполнения установленных функций, и персонала, обеспечивающего его функционирование.

Информационная система персональных данных (далее – ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Пользователь – лицо, участвующее в функционировании АС или использующее результаты ее функционирования.

4. Нормативные документы:

4.1 Стандарт разработан в соответствии с требованиями действующего законодательства Российской Федерации, требованиями регуляторов в области информационной безопасности, а также с учетом требований иных нормативных и организационно-распорядительных документов Учреждения в области информационной безопасности:

Политика информационной безопасности ГАПОУ СО «Балаковский политехнический техникум».

1. Требования к первичной идентификации пользователей

1.1. Каждому пользователю (работнику, подрядчику) присваивается уникальный идентификатор после проверки его идентификационных данных:

для работников — ФИО, должность, табельный номер;

для подрядчиков — ФИО, наименование юридического лица, номер договора.

1.2. Идентификатор должен быть уникальным и актуальным.

1.3. Регистрация идентификатора производится АИБ. В регистрации может быть отказано при:

несоответствии данных требованиям;

предоставлении недостоверных данных;

невозможности подтверждения данных;

отсутствии допуска к работе с ИС.

1.4. Для аутентификации используется аутентификация (логин + пароль).

Порядок создания, учета, изменения и блокирования, контроля, удаления учетных записей приведен в приложении №1 к настоящему стандарту.

2. Требования к моделям доступа пользователей

2.1. Применяется комбинированная модель доступа:

Ролевая (RBAC) — права привязываются к должностным ролям (преподаватель, методист, администратор ИС.).

Мандатная (MAC) — для информации с ограниченным доступом (личные дела обучающихся, персональные данные).

2.2. Принцип минимальных привилегий: пользователь получает доступ только к тем ресурсам, которые необходимы для выполнения должностных обязанностей или обучения.

2.3. Разделение обязанностей: критические операции (редактирование личных дел, изменение оценок) требуют согласования двух и более лиц.

Порядок предоставления пользователям доступа к информационным системам ГАПОУ СО «БПТ» и содержащейся в ней информации приведен в приложении №2 к настоящему стандарту.

Порядок удаленного доступа пользователей к информационным системам ГАПОУ СО «БПТ» и содержащейся в них информации приведен в приложении №3 к настоящему стандарту.

3. Перечень разрешённого и запрещённого ПО

3.1. Разрешённое ПО:

№ п/п	Описание	Наименование
Системное и прикладное программное обеспечение		
1.	Операционные системы	Microsoft Windows XP Professional SP3
2.		Microsoft Windows 7 Professional SP1
3.		Microsoft Windows 7 Ultimate SP1
4.		Microsoft Windows 8 Professional
5.		Microsoft Windows 8.1 Professional
6.		Microsoft Windows 10 Home
7.		Microsoft Windows 10 Professional
8.		Microsoft Windows 11 Home
9.		Microsoft Windows 11 Professional
10.		Microsoft Windows Server 2016
11.		Microsoft Windows Server 2019
12.		Astra Linux
13.		Linux Ubuntu
14.		РЕД ОС 7.3
15.		РЕД ОС 8
16.	Драйверы и официальные приложения для аппаратных средств	Intel
17.		AMD
18.		NVIDIA
19.		Realtek
20.		HP
21.		Lenovo
22.		Pantum
23.		Canon
24.		Kyocera
25.		Aquarius
26.		иные производители аппаратных средств

27.	Пакеты языков программирования	Microsoft Visual C++
28.		Microsoft .NET
29.		Microsoft .Net Framework
30.		Java
31.		Firebird
32.		Oracle JDK
33.	Пакеты офисных приложений	Microsoft Office 2007 Professional
34.		Microsoft Office 2007 Professional Plus
35.		Microsoft Office 2010 Professional
36.		Microsoft Office 2010 Professional Plus
37.		Microsoft Office 2016 Professional Plus
38.		Microsoft Office 2019 Standard
39.		Microsoft Office 2019 Professional
40.		Microsoft Office 2019 Professional Plus
41.		МойОфис
42.		LibreOffice
43.		AlterOffice
44.		Р7-Офис
45.	Антивирусная защита	Kaspersky Endpoint Security
46.		Dr.Web Desktop Security Suite
47.	Архиваторы	WinRar
48.		7-Zip
49.	Браузеры	Яндекс Браузер с поддержкой ГОСТ TLS;
50.		Chromium-Gost
51.	ПО для просмотра файлов «.pdf»	Adobe Acrobat Reader
52.		Adobe Acrobat Reader DC
53.		Adobe Acrobat Reader
54.		Foxit Reader
55.	ПО для редактирования файлов «.pdf»	Foxit Reader
56.		PDF24 Creator
57.	Файловые менеджеры	Total Commaner
58.	Пакеты аудио и видео кодеков	K-Lite Codec Pack
59.	Проигрыватели медиа информации	Media Player Classic
60.		VLC media player
61.		Microsoft Media Player
62.	Мессенджеры	VK Мессенджер
63.		MAX
64.	Видеоконференцсвязь	MAX
65.		Яндекс.Телемост
66.	Облачные хранилища	Яндекс.Диск
67.		Облако Mail.ru
Специализированное прикладное программное обеспечение		
68.	Бухгалтерский учет	1С: Бухгалтерия государственного учреждения
69.		1С: Зарплата и кадры государственного учреждения
70.		Свод-Смарт
71.		ПАРУС Бюджет
72.		АС «УРМ»
73.	Отечность	Документы ПУ-6
74.		Контур Экстерн

75.		1С:Отчетность
76.		Парус
77.		ПОПД ПФР
78.	Справочные системы	Гарант
79.	Видеонаблюдение и контроль доступа	AgentDVR
80.		iSpy
81.		иные системы видеонаблюдения и СКУД
82.	СКЗИ	КриптоПро CSP
83.		ViPNet Client
Специализированное прикладное программное обеспечение для образовательного процесса		
84.	Среды и средства разработки программного обеспечения	1С:Предприятие 8.3
85.		1С: EDT
86.		Microsoft Visual Studio
87.		Microsoft Visual Studio Code
88.		Intellij IDEA Community
89.		PyCharm
90.	СУБД	Microsoft SQL Server
91.		Microsoft Access
92.		SQL Server management studio
93.		PostgeSQL
94.		pgAdmin
95.	Системы контроля версий	Git (локально)
96.		Gitlab (локально)
97.	Бухгалтерский учет	1С: Бухгалтерия предприятия
98.	САПР	Компас3D v21
99.	Системы компьютерной алгебры	MathCAD

3.2. Запрещено использовать:

нелицензионное ПО;

ПО с известными уязвимостями;

мессенджеры и облачные хранилища для передачи персональных данных без согласования со структурным подразделением по защите информации;

программы для удалённого управления без разрешения АИБ.

3.3. Установка ПО производится только администратором ИС или уполномоченным работником со структурным подразделением по защите информации.

4. Требования к типовым конфигурациям и настройкам

4.1. Параметры паролей:

длина — не менее 8 символов;

сложность — 1 строчная буква, 1 строчная буква, цифра, специальный символ;

минимальный срок действия пароля – 2 дня;

максимальный срок действия пароля — 90 дней;

отличие от предыдущего пароля – 3 позиции;

запрет на повторное использование последних 5 паролей;

запрет на использование обратимого шифрования для хранения парольной информации.

Согласно Порядку парольной защиты в информационных системах персональных данных

4.2. Блокировка учётной записи после 3 неуспешных попыток входа.

4.3. Автоблокировка экрана устройства через 10 минут неактивности.

4.4. Регулярное обновление ПО и установка обновлений безопасности в течение 7 рабочих дней после выпуска.

Порядок получения, оценки, тестирования и применения обновлений программных и программно-аппаратных средств приведен в приложении №7 к настоящему стандарту.

5. Требования к доступу в интернет и удалённому доступу

5.1. Доступ в интернет:

через межсетевой экран с фильтрацией трафика и контентной фильтрацией;

блокировка доступа к сайтам с вредоносным контентом, азартными играми, соцсетям;

запрет на подключение неавторизованных Wi-Fi-устройств.

5.2. Удалённый доступ:

многофакторная аутентификация;

запрет на использование личных устройств без согласования.

Порядок предоставления пользователям доступа из информационных систем в телекоммуникационную сеть «Интернет» и контроля ее использования приведен в приложении №4 к настоящему стандарту.

6. Ограничения и запреты для пользователей

6.1. Запрещено:

передавать пароли и идентификаторы третьим лицам;

использовать съёмные носители без учёта и проверки на вирусы;

получать доступ к информации, не связанной с должностными обязанностями;

изменять конфигурации ИС без разрешения администратора;

копировать и распространять персональные данные без разрешения.

6.2. Обязательное уведомление администраторов ИС о подозрительных действиях (попытки взлома, фишинг, утечка данных).

Порядок повышения уровня знаний и информированности пользователей по вопросам защиты информации в ГАПОУ СО «БПТ» приведен в приложении №5 к настоящему стандарту.

7. Защита устройств

7.1. Конечные устройства (с постоянным доступом в интернет):

антивирус с еженедельным обновлением баз;

контроль физического доступа (запираемые помещения, видеонаблюдение).

Порядок выявления, оценки и устранения уязвимостей информационных систем приведен в приложении №5 к настоящему стандарту.

Порядок обеспечения физической защиты информационных систем приведен в приложении №8 к настоящему стандарту.

8. Резервное копирование

8.1. Копируются:

конфигурационные файлы ИС;

журналы событий.

8.2. Периодичность:

еженедельные полные копии.

8.3. Хранение:

30 дней на локальном носителе;

1 год на удалённом защищённом хранилище.

8.4. Проверка целостности копий — ежемесячно.

Порядок восстановления штатного функционирования информационных систем и тестирования процессов восстановления приведен в приложении №10 к настоящему стандарту.

9. Сбор, регистрация и анализ событий безопасности

9.1. Регистрируются:

попытки несанкционированного доступа;

изменения конфигураций ИС;

запуск подозрительных процессов и программ;

действия с персональными данными.

Порядок выявления, оценки и устранения уязвимостей информационных систем приведен в приложении №6 к настоящему стандарту.

9.2. Состав записи журнала:

дата и время;

субъект доступа (логин);

объект доступа (ресурс);

действие (чтение/запись/удаление);

результат (успех/неудача).

9.3. Срок хранения журналов — 1 год.

9.4. Анализ событий — в режиме реального времени с использованием SIEM-системы.

Порядок мониторинга информационной безопасности информационных систем приведен в приложении №11 к настоящему стандарту.

Порядок контроля уровня защищенности информации, содержащейся в информационных системах приведен в приложении №12 к настоящему стандарту.

10. Защита при подключении к внешним ИС

10.1. Каналы передачи данных:

шифрование TLS 1.3, SSL;

сетевые протоколы прикладного уровня: http, https, ftp.

10.2. Ограничение доступа к критичным данным внешних ИС: АС ИСПДн «Бухгалтерия и кадры», АС «Студенты», ФИС ФРДО, ЕТД, АИС «Зачисление в ПОО», ГИС «Профилактика».

Порядок вывода в контур промышленной эксплуатации сервисов, доступ к которым осуществляется с использованием телекоммуникационной сети «Интернет» приведен в приложении №9 к настоящему стандарту.

11. Ответственность и контроль

11.1. Обеспечение за выполнение стандарта несут:

11.1.1. Администрация Учреждения отвечает за состояние ИБ в Учреждении и обеспечивает регулярный контроль соблюдения требований настоящей Политики, актуализацию и выделение необходимых для обеспечения ИБ организационных, технических и иных ресурсов.

11.1.2. Работники, ответственные за ИБ несут ответственность за обеспечение ИБ объектов защиты информационной инфраструктуры Учреждения.

11.1.3. Руководители структурных подразделений несут ответственность за:

соблюдение работниками структурного подразделения нормам ИБ, утвержденных в Учреждении;

соответствие полномочий работников структурного подразделения по доступу к конфиденциальной информации, объектам информатизации и сетевой инфраструктуре Учреждения.

11.2. Работники Учреждения обязаны:

соблюдать требования настоящей Политики и иных нормативных и организационно-распорядительных документов Учреждения в области ИБ;

использовать информационную инфраструктуру Учреждения исключительно для выполнения своих должностных обязанностей;

информировать работников, ответственных за информационную безопасность о выявленных и/или произошедших инцидентах ИБ.

11.3. Нарушение требований настоящей Политики и иных нормативных и организационно-распорядительных документов Учреждения в области ИБ, а также сокрытие фактов произошедших инцидентов ИБ работниками Учреждения запрещается.

11.4. Работники Учреждения, наущающие и/или не выполняющие требования настоящей Политики или требования иных организационно-распорядительных документов Учреждения в области ИБ, несут ответственность, установленную действующим законодательством Российской Федерации.

работники иных структурных подразделений Учреждения, обучающиеся — соблюдение правил работы с информацией.

11.5. Контроль исполнения:

плановые проверки — 1 раз в год;

внеплановые проверки — при выявлении нарушений, а также событий и/или инцидентов ИБ.

12. Порядок внесения изменений

12.1. Пересмотр стандарта — не реже 1 раза в год или при:

изменении законодательства;

внедрении новых ИС;

выявлении новых угроз ИБ;

изменении структуры

Приложение № 1
к Внутреннему стандарту по защите информации

Порядок создания, учета, изменения и блокирования, контроля, удаления учетных записей

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Порядок создания, учета, изменения и блокирования, контроля, удаления учетных записей (далее – Порядок) разработан с целью определения правил управления учетными записями от персональных электронных вычислительных машин, информационных и автоматизированных систем, а также иных объектов информатизации, находящихся в эксплуатации в ГАПОУ СО «Балаковский политехнический техникум» (далее – Учреждение).

1.2. Настоящий Порядок является неотъемлемой частью организационных мер по обеспечению информационной безопасности на объектах информатизации Учреждения и входит в состав общих организационно-распорядительных мер, реализующихся в рамках Политики информационной безопасности Учреждения.

1.3. Порядок направлен на повышение эффективности мер по:

– защищенности информации, обрабатываемой на объектах информатизации Учреждения;

– минимизации вероятности несанкционированного и/или неправомерного доступа, модификации, копирования, распространения, блокирования и уничтожения информации, обрабатываемой на объектах информатизации Учреждения.

1.4. Настоящий Порядок регламентирует следующие стадии управления учетными записями:

– создание учетных записей;

– контроль учетных записей;

– изменение учетных записей;

– блокирование учетных записей;

– удаление учетных записей.

1.5. Настоящий Порядок не регламентирует параметры качества идентификационной и/или аутентификацонной информации учетных записей.

1.6. Настоящий Порядок не регламентирует организацию и порядок доступа работников к информационным системам Учреждения.

1.7. Непосредственное исполнение положений настоящего Порядка осуществляет Администратор информационной системы.

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1. Требования настоящего Порядка распространяются на:

– информационные системы персональных данных, эксплуатируемые в Учреждении;

– автоматизированные рабочие места;

– работников Учреждения, использующих при выполнении своих должностных и функциональных обязанностей автоматизированные рабочие места, информационные системы персональных данных и/или обращающихся к информации, обрабатываемой в таких системах.

2.2. Требования Порядка не распространяются на персональные электронно-вычислительные машины не являющимися автоматизированными рабочими местами.

3. ПОРЯДОК ИСПОЛЬЗОВАНИЯ УЧЕТНЫХ ЗАПИСЕЙ

3.1. С целью соблюдения принципа персональной ответственности за свои действия, каждому работнику, допущенному к работе с ИС, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в системе.

4. ПОРЯДОК СОЗДАНИЯ УЧЕТНЫХ ЗАПИСЕЙ

4.1. Процесс создания учетных записей для внутренних пользователей предусматривает следующий порядок:

– создание учетных записей;

– присвоение роли и прав доступа;

– предоставление доступа к отдельным компонентам ИС;

– информирование о результатах создания учетных записей.

4.2. Допуск работника к работе в ИС

4.2.1. Процедура создания учетной записи внутреннего пользователя и предоставления ему прав доступа к ресурсам ИС инициируется заявкой работника на предоставление доступа к ИС на основании приказа директора Учреждения о допуске работника к работам в ИС.

4.2.2. Условия и порядок предоставления доступа пользователям к ИС регламентируется Порядком предоставления пользователям доступа к информационным системам ГАПОУ СО «БПТ» и содержащейся в ней информации.

4.3. Создание учетной записи

4.3.1. Работник, ответственный за ИБ создает учетную запись пользователя в каталоге учетных записей операционной системы и/или информационной системы на АРМ пользователя в соответствии с заявкой.

4.3.2. В соответствии с требованиями внутреннего документа Порядок парольной защиты в информационных системах персональных данных Государственного автономного профессионального образовательного учреждения Саратовской области «Балаковский политехнический техникум», работник, ответственный за информационную безопасность создает первоначальную аутентификационную (парольную) информацию для прохождения успешной первичной аутентификации в ИС.

4.4. Присвоение прав доступа учетной записи

4.4.1. Созданная учетная запись ограничивается минимальным набором прав доступа, позволяющих пользователю осуществлять надлежащее выполнение трудовых (должностных) и функциональных обязанностей пользователя при эксплуатации ИС.

4.5. Информирование о результатах

4.5.1. Работник, ответственный за ИБ уведомляет пользователя о результатах выполнения заявки лично в устном виде, передавая присвоенную первичную идентификационную и аутентификационную информацию пользователю.

4.6. Процесс создания учетной записи пользователя не должен превышать трех рабочих дней от даты согласования заявки.

5. ПОРЯДОК ИЗМЕНЕНИЯ УЧЕТНЫХ ЗАПИСЕЙ

5.1. Изменение действующей учетной записи пользователя возможно в следующих случаях:

– изменение выполняемых пользователем должностных или функциональных обязанностей;

– изменение занимаемой должности или подразделения пользователя.

5.2. В случае наличия внутренних распорядительных актов Учреждения, попадающих под действие пункта 5.1 настоящего Порядка, работник, ответственный за ИБ вносит изменения в учетную запись пользователя согласно новой информации.

5.3. Смена идентификационной информации

5.3.1. Идентификационная информация, включая идентификаторы доступа не могут быть изменены в течение всего жизненного цикла учетной записи, за исключением случаев, когда идентификатор учетной записи присвоен учетной записи по ошибке или была допущена ошибка в символьном наборе идентификатора учетной записи.

5.4. Смена аутентификационной (парольной) информации

5.4.1. Смена аутентификационной (парольной) информации учетной записи пользователя выполняется пользователем самостоятельно или с привлечением работников Учреждения, ответственных за ИБ.

5.4.2. Смена аутентификационной (парольной) информации учетной записи пользователя не требует согласования и выполняется в соответствии с требованиями внутреннего документа Учреждения «Порядок парольной защиты в информационных системах персональных данных

Государственного автономного профессионального образовательного учреждения Саратовской области «Балаковский политехнический техникум».

5.5. Изменение прав доступа

5.5.1. Права доступа могут быть изменены в случае, если:

– текущий набор прав доступа учетной записи не соответствует необходимому минимальному набору прав доступа для надлежащего выполнения трудовых (должностных) обязанностей пользователя;

– текущий набор прав доступа учетной записи избыточен и/или излишне привилегирован.

5.5.2. Работник, ответственный за ИБ изменяет права доступа учетной записи с учетном предоставления минимально возможных привилегий.

6. ПОРЯДОК БЛОКИРОВАНИЯ УЧЕТНЫХ ЗАПИСЕЙ

6.1. Блокирование учетных записей пользователей является процедурой временных ограничений, которые налагаются на учетные записи пользователей. Блокирование учетных записей является обратимой процедурой, при которой осуществление взаимодействия пользователей с заблокированными учетными записями невозможно в течение всего периода блокирования.

6.2. Блокирование учетных записей пользователей выполняется работниками, ответственными за ИБ в следующих случаях:

– при компрометации идентификационной, аутентификационной информации и/или иной информации ограниченного доступа в случае, если внесение изменений в учетную запись заведомо не приведет к ликвидации компрометирующих событий;

– при выявлении злоупотребления пользователем правами доступа учетной записи;

– изменение выполняемых пользователем должностных или функциональных обязанностей;

– изменение занимаемой должности или подразделения пользователя.

– при несоблюдении работником требований нормативно-правовых актов учреждения в области защиты ИБ.

7. ПОРЯДОК УДАЛЕНИЯ УЧЕТНЫХ ЗАПИСЕЙ

7.1. Удаление учетных записей пользователей является безвозвратной процедурой, при которой все данные и информация, принадлежащие удаляемой учетной записи полностью уничтожаются.

7.2. Удаление учетных записей пользователей выполняется работниками, ответственными за ИБ в следующих случаях:

– увольнение работника;

– при ошибочно созданной учетной записи или обнаруженных неиспользуемых учетных записях.

8. ПОРЯДОК КОНТРОЛЯ УЧЕТНЫХ ЗАПИСЕЙ

8.1. Контроль учетных записей выполняется работниками, ответственными за ИБ в следующих целях:

– контроль состояния учетной записи;

– выявление иных (незаявленных) пользовательских учетных записей, в том числе неактивных учетных записей;

– выявление идентификационной информации и идентификаторов учетных записей пользователей, не соответствующих требованиям внутренних нормативных документов в области ИБ;

– выявление аутентификационной информации учетных записей, не соответствующих требованиям внутренних нормативных документов в области ИБ;

– выявление прав доступа учетных записей, не соответствующих требованиям внутренних нормативных документов Учреждения в области ИБ;

– выявление наличия гостевых учетных записей.

8.2. В случае, если в результате контроля учетных записей были обнаружены учетные записи, попадающие под действие пункта 8.1 настоящего Порядка, работник, ответственный за ИБ должен предпринять меры по изменению, блокированию или удалению таких учетных записей.

8.3. Периодичность контроля

8.3.1. Плановый контроль учетных записей выполняется не реже одного раза в три месяца, при этом охват планового контроля должен охватывать все имеющиеся в ИС учетные записи пользователей.

8.3.2. Внеплановый контроль выполняется в следующих случаях:

– кадровые события, связанные с трудоустройством, переводом на другую должность и увольнением работников;

– поступление информации о злоупотреблении пользователем назначенными ему в учетной записи правами;

– поступление информации о несоблюдении пользователем требований внутренних нормативно-правовых документов в области ИБ;

– выявление событий и/или инцидентов ИБ;

9. ОТВЕТСТВЕННОСТЬ

9.1 Пользователи и работники, ответственные за ИБ несут ответственность за нарушение требований настоящего Порядка в соответствии с законодательством Российской Федерации, локальными нормативно-правовыми актами Учреждения и условиями заключенных договоров.

9.2 Работники, ответственные за ИБ, несут ответственность за организацию контроля и соблюдение настоящего Порядка в пределах их компетенции.

10. ПОРЯДОК ПЕРЕСМОТРА НАСТОЯЩЕГО ПОРЯДКА

10.1 Настоящий Порядок подлежит пересмотру:

– при изменении законодательства Российской Федерации и обязательных требований в области защиты информации;

– при изменении структуры, состава и условий функционирования информационных систем Учреждения;

– при изменении требований ИБ, предъявляемых к идентификации и аутентификации пользователей в информационных системах.

– при изменении локальных нормативно-правовых актов Учреждения в области ИБ;

– по результатам контроля, проверок, аудитов и расследования инцидентов ИБ.

10.2 Плановый пересмотр настоящего Порядка осуществляется не реже одного раза в 3 года.

10.3 Подготовку предложений по актуализации настоящего Порядка организуют работники, ответственные за ИБ.

Приложение № 2
к Внутреннему стандарту по защите информации

Порядок предоставления пользователям доступа к информационным системам ГАПОУ СО «БПТ» и содержащейся в ней информации

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Порядок предоставления пользователям доступа к информационным системам ГАПОУ СО «БПТ» и содержащейся в них информации (далее – Порядок) определяет условия, основания, состав, порядок предоставления, изменения, пересмотра, приостановления и прекращения доступа пользователей к информационным системам ГАПОУ СО «Балаковский политехнический техникум» (далее – Учреждение) и содержащейся в них информации.

1.2 Настоящий Порядок является локальным нормативным актом Учреждения в области защиты информации и обязателен для исполнения работниками Учреждения, а также иными лицами, которым в установленном порядке предоставляется доступ к информационным системам Учреждения и содержащейся в них информации.

1.3 Настоящий Порядок разработан в целях:

– обеспечения правомерного и контролируемого доступа к информационным системам Учреждения и содержащейся в них информации;

– исключения несанкционированного доступа к информационным системам Учреждения и содержащейся в них информации;

– разграничения прав доступа пользователей в соответствии с их должностными обязанностями и служебной необходимостью;

– обеспечения контроля использования предоставленных прав доступа;

– соблюдения требований локальных нормативных актов Учреждения в области защиты информации.

1.4 Предоставление доступа к информационным системам Учреждения и содержащейся в них информации осуществляется на основании следующих принципов:

– законности;

– обоснованности и служебной необходимости;

– минимально необходимого объема прав доступа;

– персональной ответственности пользователя;

– разграничения прав доступа;

– обязательности контроля предоставленного доступа и действий пользователей.

1.5 Настоящий Порядок регулирует:

– порядок предоставления доступа внутренним пользователям к информационным системам Учреждения и содержащейся в них информации;

– порядок предоставления доступа работникам подрядных организаций к информационным системам Учреждения и содержащейся в них информации;

– порядок предоставления доступа работникам иных государственных органов, организаций к информационным системам Учреждения и содержащейся в них информации;

– порядок изменения, пересмотра, приостановления и прекращения доступа;

– порядок контроля предоставленного доступа.

1.6 Порядок удаленного доступа к информационным системам Учреждения и содержащейся в них информации определяется отдельным локальным нормативным актом Учреждения.

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1 Требования настоящего Порядка распространяются на:

– федеральные, государственные, объектовые и иные информационные системы Учреждения;

– автоматизированные рабочие места, серверы, виртуальные машины, иные программные и программно-аппаратные средства, входящие в состав информационных систем Учреждения;

– работников Учреждения, использующих информационные системы Учреждения и содержащуюся в них информацию;

– работников подрядных организаций, которым в установленном порядке предоставляется доступ к информационным системам Учреждения и содержащейся в них информации;

– работников иных государственных органов, организаций, которым в установленном порядке предоставляется доступ к информационным системам Учреждения и содержащейся в них информации;

– работников, ответственных за ИБ;

– работников Учреждения, обеспечивающих эксплуатацию информационных систем Учреждения.

2.2 Требования настоящего Порядка применяются при:

– первичном предоставлении доступа;

– изменении состава и объема прав доступа;

– пересмотре предоставленных прав доступа;

– временном ограничении доступа;

– приостановлении и прекращении доступа;

– контроле использования информационных систем Учреждения и содержащейся в них информации.

3. КАТЕГОРИИ ПОЛЬЗОВАТЕЛЕЙ

3.1 Для целей настоящего Порядка устанавливаются следующие категории пользователей:

– внутренние пользователи;

– пользователи из числа работников подрядных организаций;

– пользователи из числа работников иных государственных органов, организаций.

3.2 Внутренними пользователями являются работники Учреждения, которым в связи с исполнением должностных обязанностей предоставляется доступ к информационным системам Учреждения и содержащейся в них информации.

3.3 Пользователями из числа работников подрядных организаций являются работники организаций, привлекаемых Учреждением для оказания услуг, выполнения работ по обработке, хранению информации, созданию, развитию, сопровождению, обеспечению эксплуатации информационных систем Учреждения, а также для выполнения работ и оказания услуг по защите информации.

3.4 Пользователями из числа работников иных государственных органов, организаций являются лица, не состоящие в трудовых отношениях с Учреждением и не являющиеся работниками подрядных организаций, которым в установленном порядке может быть предоставлен доступ к информационным системам Учреждения и содержащейся в них информации.

4. УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ИС

4.1 Основанием для предоставления пользователю доступа к информационным системам Учреждения и содержащейся в них информации является документально подтвержденная служебная необходимость.

4.2 Доступ предоставляется только в объеме, необходимом для выполнения трудовых (должностных) обязанностей, функций или работ, предусмотренных документами Учреждения, договором, соглашением или иным правовым основанием.

4.3 Предоставление внутреннему пользователю доступа к ИС, находящейся в стадии эксплуатации осуществляется путем создания учетной записи внутреннего пользователя в ИС, согласно Порядку создания, учета, изменения и блокирования, контроля, удаления учетных записей.

4.4 В случае наличия основания для предоставления доступа к ИС, в предоставлении доступа к ИС внутреннему пользователю может быть отказано в следующих случаях:

– в заявке на предоставление доступа к ИС указана неполная, неточная, недостоверная информация и/или информация полноту, точность и/или достоверность невозможно подтвердить;

– нарушение порядка или маршрута согласования заявки на предоставление доступа к ИС;

– отсутствие у внутреннего пользователя соответствующих полномочий на выполнение трудовых обязанностей, связанных с обработкой данных, находящихся в ИС или на обращения к таким данным.

4.5 В случае отказа внутреннему пользователю в доступе к ИС, внутренний пользователь обязательно уведомляется об отказе в предоставлении доступа к ИС, в том числе о причинах такого отказа в устном или письменном виде руководителем структурного подразделения или директором Учреждения.

5. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ИС ВНУТРЕННИМ ПОЛЬЗОВАТЕЛЯМ

5.1 Основанием для предоставления внутреннему пользователю доступа к ИС Учреждения и содержащейся в них информации является:

– приказ о приеме работника в Учреждение или иной документ, подтверждающий возникновение трудовых отношений;

– наличие должностных обязанностей, предусматривающих необходимость доступа;

– ознакомление работника с локальными нормативно-правовым актами Учреждения в области ИБ в части, его касающейся;

– оформленная и согласованная заявка на предоставление доступа к ИС.

5.2 В заявке на предоставление доступа к ИС внутреннему пользователю указываются:

– наименование ИС, к которой необходимо предоставить доступ;

– компоненты или компоненты ИС, к которым необходимо предоставить доступ;

–требование в привилегированном доступе к ИС;

– основание для подключения;

– фамилия, имя и отчество работника;

– структурное подразделение;

– должность, согласно штатному расписанию;

– табельный номер работника;

– номер телефона работника;

– инвентарный номер АРМ;

– компоненты, к которым будут ограничены права пользователя;

– антивирусное ПО;

– специальное ПО.

5.3 Заявка подлежит согласованию:

– работником, ответственным за ИБ;

– директором Учреждения.

5.4 Предоставление внутренним пользователям доступа к ИС осуществляется в следующем порядке:

1. сформированная работником заявка на предоставление доступа к ИС направляется работнику, ответственному за ИБ;

2. согласованная с работником, ответственным за ИБ заявка на предоставление доступа к ИС направляется директору Учреждения;

3. после рассмотрения заявки, директор Учреждения утверждает решение о предоставлении доступа к внутреннему пользователю доступа к ИС, при этом на бланке заявки указывается дата согласования и личная подпись директора Учреждения;

4. администратор ИС, в течение трех рабочих дней с момента согласования заявки создает учетную запись пользователя в соответствии с Порядком создания, учета, изменения и блокирования, контроля, удаления учетных записей, предварительно осуществив настройку

программно-аппаратной части ПЭВМ, телекоммуникационных средств, средств антивирусной защиты и СЗИ, в том числе СЗИ от НСД и т.д.;

5.5 Срок действия и хранение заявки на предоставление доступа к ИС

5.5.1 Датой начала действия заявки на предоставление доступа к ИС является дата, указанная директором при ее согласовании.

5.5.2 Согласованная заявка на предоставление доступа к ИС считается выполненной по истечении трех рабочих дней с момента подписания заявки или при фактическом создании учетной записи согласно заявке.

5.5.3 Согласованная заявка на предоставление доступа к ИС не имеет срока окончания действия и действует на протяжении всего периода выполнения работником трудовых (должностных) обязанностей, связанных с обработкой информации в ИС или получением возможности работником ознакомляться с такой информацией.

5.5.4 Заявка передается на хранение работникам, ответственным за ИБ, при этом заявка должна храниться в сейфе или шкафу, запирающимся на ключ в течение всего периода действия текущего доступа внутреннего пользователя к ИС и в течение одного года после отключения пользователя от ИС.

6. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОСТУПА К ИС ДЛЯ ВНЕШНИХ ПОЛЬЗОВАТЕЛЕЙ

6.1 Предоставление доступа внешнему пользователю к ИС Учреждения осуществляется на основании соглашения между Учреждением и организацией внешнего пользователя (подрядной организацией) об информационном обмене при предоставлении услуг, в котором обязательно указывается:

– ИС, доступ к которой предоставляется внешнему пользователю;

– метод подключения;

– физическое расположение ИС;

– состав и содержание информации, доступ к которой предоставляется;

– перечень предоставляемых услуг, в части эксплуатации внешним пользователем ИС Учреждения;

– порядок предоставления доступа внешнему пользователю к ИС;

– порядок и условия прекращения предоставления доступа внешнему пользователю к ИС;

– требования по обеспечению безопасности информации;

– срок, в течение которого будет предоставляться доступ к ИС, в том числе дни недели, по которым доступ будет предоставляться с указанием временного промежутка предоставления доступа;

6.2 Также обязательно указываются следующие обязательства организация внешнего пользователя:

– обеспечивать сохранность, доступность, целостность и неизменность информации, обрабатываемой в ИС Учреждения;

– обеспечивать исключение несанкционированного использования, сбора, записи, систематизации, накопления, модификации, подмены, распространения (в том числе передачи информации, доступ к которой предоставляется внешнему пользователю третьей стороне без предварительного согласования с Учреждением), блокирования и/или уничтожения любых видов информации, доступ к которым предоставляется на основании соглашения;

– обеспечивать исключение распространения и утечек информации ограниченного доступа и иной конфиденциальной информации, обрабатываемой в ИС;

– обеспечивать исключение распространения и утечек персональных данных, обрабатываемых в ИС;

– обеспечить соблюдение требований Политики информационной безопасности ГАПОУ СО «БПТ»;

– обеспечивать выполнение требований в области ИБ, установленных нормативно-правовыми актам Учреждения.

6.3 Порядок предоставления доступа к ИС для внешнего пользователя указывается подробно описывается в тексте соглашение об информационном обмене при предоставлении услуг.

6.4 В случае невозможности исполнения обязательств организацией внешнего пользователя, предусмотренных соглашением, она обязана незамедлительно уведомить о таком случае директора Учреждения.

6.5 Перед подписанием, соглашение об информационном обмене при предоставлении услуг обязательно согласовывается с работниками, ответственными за ИБ.

6.6 В течение всего срока предоставления внешнему пользователю доступа к ИС Учреждения и/или предоставления доступа к информации, обрабатываемой в ИС Учреждении обязательно должен вестись постоянный контроль лицами, ответственными за внесение данных в ИС и/или работниками, ответственными за ИБ.

6.7 Контроль за предоставленным внешнему пользователю доступом и приемка выполненных работ осуществляется работниками, ответственными за эксплуатацию ИС, в следующих случаях:

– услуги, предоставляемые внешним пользователем на основании соглашения частично или полностью связаны с обработкой данных и/или выполнением функций, предусмотренных процессами нормальной эксплуатации ИС;

– услуги, предоставляемые внешним пользователем на основании соглашения частично или полностью связаны с консультированием и/или информированием внутренних пользователей об особенностях работы конкретного программного обеспечения, входящего в состав ИС.

6.8 Контроль за предоставленным внешнему пользователю доступом и приемка выполненных работ осуществляется работниками, ответственными за ИБ во всех случаях, когда услуги, предоставляемые внешним пользователем на основании соглашения частично или полностью связаны с проведением работ, связанных изменением состава и/или параметров работы (функционирования) программно-аппаратной части ИС.

7. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОСТУПА РАБОТНИКАМ ИНЫХ ГОСУДАРСТВЕННЫХ ОРГАНОВ, ОРГАНИЗАЦИЙ

7.1 На постоянной основе доступ работникам иных государственных органов, организаций к ИС Учреждения и содержащейся в них информации не предоставляется.

7.2 В Учреждении отсутствуют действующие процессы предоставления работникам иных государственных органов, организаций доступа к информационным системам Учреждения и содержащейся в них информации.

7.3 В случае возникновения документально подтвержденной необходимости доступ работникам иных государственных органов, организаций может быть предоставлен только:

– на основании отдельного решения директора Учреждения;

– при наличии правового, организационного или договорного основания;

– после определения информационной системы Учреждения, состава информации, объема прав доступа, срока действия доступа, порядка контроля и прекращения доступа;

– после согласования с работниками, ответственными за ИБ.

7.4 До фактического предоставления такого доступа должны быть определены:

– необходимость и правомерность предоставления доступа;

– перечень пользователей;

– объем прав доступа;

– меры защиты информации;

– порядок контроля использования предоставленного доступа;

– порядок прекращения доступа.

8. ПОРЯДОК ИЗМЕНЕНИЯ, ПЕРЕСМОТРА, ПРИОСТАНОВЛЕНИ И ПРЕКРАЩЕНИЯ ПРЕДОСТАВЛЕНИЯ ПОЛЬЗОВАТЕЛЮ ДОСТУПА К ИС

8.1 Предоставленные пользователю права доступа подлежат пересмотру:

– при изменении должности, функций или полномочий пользователя;

– при переводе пользователя в другое структурное подразделение;

– при изменении состава задач, выполняемых подрядной организацией;

– при изменении состава и структуры информационной системы Учреждения;

– по результатам проверок, контроля и аудита;

– при выявлении нарушений требований защиты информации;

– по окончании срока временного доступа.

8.2 Изменение или ограничение прав доступа осуществляется на основании заявки, служебной записки, решения работников, ответственны за ИБ, решения директора Учреждения либо по результатам контроля.

8.3 Доступ подлежит приостановлению или прекращению в случаях:

– увольнения работника Учреждения;

– прекращения действия договора, контракта или соглашения с подрядной организацией;

– отпадения служебной необходимости;

– выявления нарушений требований защиты информации;

– возникновения инцидента информационной безопасности;

– компрометации аутентификационной информации;

– окончания срока предоставленного доступа;

– принятия соответствующего решения директором Учреждения или работников, ответственных за ИБ.

8.4 При прекращении доступа должны быть выполнены действия по:

– блокированию или удалению учетной записи;

– отзыву или изменению прав доступа;

– изъятию или аннулированию аутентификационной информации и средств доступа;

– документальному фиксированию прекращения доступа.

9. КОНТРОЛЬ ПРЕДОСТАВЛЕННОГО ДОСТУПА

9.1 Контроль предоставления и использования доступа к информационным системам Учреждения и содержащейся в них информации осуществляется работниками, ответственными за ИБ, а также работниками Учреждения, обеспечивающими эксплуатацию информационных систем, в пределах установленной компетенции.

9.2 Контроль включает:

– учет пользователей и их прав доступа;

– учет оснований предоставления доступа;

– контроль актуальности предоставленных прав;

– анализ событий доступа;

– выявление избыточных, неиспользуемых и неправомерно используемых прав доступа;

– проверку соблюдения пользователями установленных ограничений.

9.3 Все действия по предоставлению, изменению, пересмотру, приостановлению и прекращению доступа подлежат документированию.

9.4 Периодичность и порядок проверки актуальности предоставленных прав доступа определяются Учреждением.

10. ПРАВА И ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ

10.1 Пользователь обязан:

– использовать предоставленный доступ исключительно в пределах своих трудовых (должностных) обязанностей, функций или работ;

– соблюдать требования локальных нормативно-правовых актов Учреждения в области ИБ;

– не передавать свои учетные данные и средства доступа другим лицам;

– не предпринимать действий, направленных на получение несанкционированного доступа;

– незамедлительно сообщать о выявленных нарушениях и признаках инцидентов информационной безопасности.

10.2 Пользователю запрещается:

– использовать предоставленные права доступа не по назначению;

– получать доступ к информации, для которой он не уполномочен;

– копировать, изменять, удалять, передавать информацию с нарушением установленных требований;

– обходить установленные механизмы защиты информации;

– использовать чужие учетные записи или предоставлять свою учетную запись другим лицам.

11. ОТВЕТСТВЕННОСТЬ

11.1 Пользователи несут ответственность за нарушение требований настоящего Порядка в соответствии с законодательством Российской Федерации, локальными нормативно-правовыми актами Учреждения и условиями заключенных договоров.

11.2 Руководители структурных подразделений Учреждения несут ответственность за обоснованность инициирования предоставления доступа и своевременное информирование об изменении служебной необходимости.

11.3 Работники, ответственные за ИБ несут ответственность за организацию контроля и соблюдение настоящего Порядка в пределах компетенции.

12. ПОРЯДОК ПЕРЕСМОТРА НАСТОЯЩЕГО ПОРЯДКА

12.1 Настоящий Порядок подлежит пересмотру:

– при изменении законодательства Российской Федерации и обязательных требований в области защиты информации;

– при изменении структуры, состава и условий функционирования информационных систем Учреждения;

– при изменении локальных нормативно-правовых актов Учреждения в области ИБ;

– по результатам контроля, проверок, аудитов и расследования инцидентов ИБ.

12.2 Плановый пересмотр настоящего Порядка осуществляется не реже одного раза в три года.

12.3 Подготовку предложений по актуализации настоящего Порядка организуют работники, ответственные за ИБ.

Приложение № 1
к Порядку предоставления пользователям доступа к
информационным системам ГАПОУ СО «БПТ» и
содержащейся в ней информации

Форма заявки на предоставление доступа к информационной системе

ЗАЯВКА
на предоставление доступа к информационной системе

<table>
<tr><td>Информационная система
(нужное отметить)</td><td colspan="2">□ ФИС ФРДО
□ ФИС «ГИА и Приема»
□ ГИС «Профилактика»
□ АИС «Зачисление ПОО»
□ АС «Бухгалтерия и кадры»
□ АС «Студенты»
□ ЕТД</td></tr>
<tr><td>Компонент ИС</td><td colspan="2"></td></tr>
<tr><td>Требование в привилегированном доступе к ИС (да/нет)</td><td colspan="2"></td></tr>
<tr><td>Основание для подключения</td><td colspan="2"></td></tr>
<tr><td>Фамилия, имя, отчество</td><td colspan="2"></td></tr>
<tr><td>Структурное подразделение</td><td colspan="2"></td></tr>
<tr><td rowspan="2">Должность, табельный номер</td><td>Должность</td><td>Табельный номер</td></tr>
<tr><td></td><td></td></tr>
<tr><td>Номер телефона</td><td colspan="2"></td></tr>
<tr><td colspan="3">Заполняется работником, ответственным за ИБ</td></tr>
<tr><td>Инвентарный номер АРМ</td><td colspan="2"></td></tr>
<tr><td>Ограничения прав пользователя (указываются компоненты)</td><td colspan="2"></td></tr>
<tr><td>Антивирусное ПО</td><td colspan="2"></td></tr>
<tr><td>Специальное ПО</td><td colspan="2"></td></tr>
</table>

Фамилия, имя, отчество работника _____ _____
(личная подпись, дата) (расшифровка подписи)

Работник, ответственный за информационную безопасность _____ _____
(личная подпись, дата) (расшифровка подписи)

Директор ГАПОУ СО «БПТ»: _____ _____
(личная подпись, дата) (расшифровка подписи)

Приложение № 3
к Внутреннему стандарту по защите информации

Порядок удаленного доступа пользователей к информационным системам ГАПОУ СО «БПТ» и содержащейся в них информации

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Порядок удаленного доступа пользователей к информационным системам ГАПОУ СО «БПТ» (далее – Учреждение) и содержащейся в них информации (далее – Порядок) определяет условия, основания, ограничения и порядок предоставления удаленного доступа к информационным системам Учреждения и содержащейся в них информации.

1.2 Настоящий Порядок является обязательным для исполнения работниками Учреждения, а также иными лицами, которым в установленном порядке предоставляется удаленный доступ к информационным системам Учреждения и содержащейся в них информации.

1.3 Настоящий Порядок разработан в целях:

– исключения несанкционированного доступа к информационным системам Учреждения и содержащейся в них информации при удаленном подключении;

– обеспечения защиты каналов передачи данных;

– обеспечения защиты программных и программно-аппаратных средств, используемых для удаленного доступа;

– обеспечения контроля удаленного доступа пользователей.

1.4. Удаленный доступ предоставляется только при наличии документально подтвержденной служебной необходимости и невозможности либо существенной затрудненности выполнения соответствующих функций без такого доступа.

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1. Требования настоящего Порядка распространяются на:

– удаленный доступ работников Учреждения к информационным системам Учреждения и содержащейся в них информации;

– удаленный доступ работников подрядных организаций, если такой доступ предусмотрен документами Учреждения;

– программные и программно-аппаратные средства, используемые для удаленного доступа;

– каналы передачи данных, используемые для удаленного доступа;

– работников ответственных за ИБ и работников, обеспечивающих эксплуатацию информационных систем Учреждения.

3. ОБЩИЕ ТРЕБОВАНИЯ К УДАЛЕННОМУ ДОСТУПУ

3.1 Удаленный доступ пользователей к информационным системам Учреждения и содержащейся в них информации в целях выполнения своих обязанностей должен осуществляться:

– с использованием телекоммуникационных сетей и/или сетей связи, расположенных на территории Российской Федерации;

– с применением средств защиты канала передачи данных;

– с применением строгой аутентификации пользователей.

3.2 При удаленном доступе должны приниматься меры по защите:

– ИС Учреждения и содержащейся в них информации;

– каналов передачи данных;

– программных и программно-аппаратных средств, с использованием которых осуществляется удаленный доступ;

– удаленно подключаемого программно-аппаратного средства пользователя от несанкционированного доступа.

3.3 Удаленный доступ в целях выполнения обязанностей должен осуществляться с использованием программных и программно-аппаратных средств, выделенных Учреждением и соответствующих установленным требованиям.

3.4 Использование личных программных и программно-аппаратных средств пользователя для удаленного доступа допускается только:

– по согласованию с работниками, ответственными за ИБ;

– при наличии у Учреждения возможности контроля использования таких средств;

– при применении сертифицированных средств обеспечения безопасной дистанционной работы;

– при применении средств антивирусной защиты;

– при применении иных средств защиты информации, исключающих угрозы безопасности информации, связанные с удаленным доступом.

3.5 Удаленный доступ, не связанный с выполнением пользователем своих обязанностей, в том числе к общедоступной информации, не допускается, если иное не установлено отдельным решением Учреждения.

4. КАТЕГОРИИ УДАЛЕННОГО ДОСТУПА

4.1 В Учреждении устанавливаются следующие категории удаленного доступа:

– удаленный доступ работников Учреждения;

– удаленный доступ работников подрядных организаций;

– удаленный привилегированный доступ.

4.2 Удаленный доступ работников иных государственных органов, организаций на постоянной основе не предоставляется.

4.3 В случае возникновения документально подтвержденной необходимости удаленный доступ работникам иных государственных органов, организаций может быть предоставлен только по отдельному решению директора Учреждения при соблюдении требований настоящего Порядка.

5. ОСНОВАНИЯ И ПОРЯДОК ПРЕДОСТАВЛЕНИЯ УДАЛЕННОГО ДОСТУПА РАБОТНИКАМ УЧРЕЖДЕНИЯ

5.1 Основанием для предоставления работнику Учреждения удаленного доступа является:

– документально подтвержденная служебная необходимость;

– согласованная заявка на предоставление удаленного доступа;

– наличие выделенного Учреждением программного или программно-аппаратного средства для удаленного доступа либо отдельное согласование использования личного средства.

5.2 В заявке на предоставление удаленного доступа указываются:

– фамилия, имя, отчество пользователя;

– должность;

– структурное подразделение Учреждения;

– наименование информационной системы Учреждения;

– состав информации, к которой требуется удаленный доступ;

– объем прав доступа;

– вид удаленного доступа;

– используемое средство удаленного доступа;

– срок предоставления удаленного доступа;

– режим предоставления удаленного доступа;

– обоснование необходимости.

5.3 Заявка подлежит согласованию:

– работником, ответственным за ИБ;

– директором Учреждения.

5.4 После согласования заявки удаленный доступ предоставляется путем:

– создания или восстановления соответствующей учетной записи;

– настройки средств удаленного доступа;

– назначения прав доступа;

– доведения до пользователя требований безопасного использования удаленного доступа.

6. УДАЛЕННЫЙ ДОСТУП РАБОТНИКОВ ПОДРЯДНЫХ ОРГАНИЗАЦИЙ

6.1 Удаленный доступ работникам подрядных организаций допускается только при наличии документов Учреждения, являющихся основанием для выполнения работ или оказания услуг, и только в объеме, необходимом для их выполнения.

6.2 В документах Учреждения должны быть определены:

– основания и цели удаленного доступа;

– конкретные пользователи;

– используемые средства удаленного доступа;

– объем и срок доступа;

– меры защиты информации;

– порядок контроля действий пользователей;

– порядок прекращения удаленного доступа.

6.3 Удаленный доступ работников подрядных организаций должен быть персонализированным, ограниченным по времени и контролируемым.

6.4 Не допускается копирование подрядной организацией информации, к которой ей предоставлен удаленный доступ, если такое копирование прямо не предусмотрено документами Учреждения.

7. ТРЕБОВАНИЯ К СРЕДСТВАМ И УСЛОВИЯМ УДАЛЕННОГО ДОСТУПА

7.1 Средства удаленного доступа, применяемые в Учреждении, должны соответствовать требованиям локальных нормативных актов Учреждения в области защиты информации и утвержденным внутренним стандартам по конфигурациям и настройкам.

7.2 При удаленном доступе обязательно должны обеспечиваться:

– защита канала передачи данных;

– строгая аутентификация пользователя;

– защита удаленно подключаемого средства пользователя;

– регистрация действий пользователей и событий безопасности;

– ограничение объема прав доступа минимально необходимым объемом.

7.3 Для удаленного привилегированного доступа дополнительно должны применяться повышенные меры контроля, аутентификации и регистрации действий.

7.4 Пользователь обязан исключить несанкционированный доступ к программному или программно-аппаратному средству, с использованием которого осуществляется удаленный доступ.

7.5 При использовании личного средства пользователя до предоставления доступа должны быть проверены и подтверждены:

– наличие согласования;

– наличие необходимых средств защиты информации;

– возможность контроля использования такого средства со стороны Учреждения.

8. КОНТРОЛЬ УДАЛЕННОГО ДОСТУПА

8.1 Контроль удаленного доступа пользователей к ИС Учреждения осуществляется в соответствии с внутренними стандартами и регламентами по защите информации.

8.2 Контроль включает:

– учет пользователей, которым предоставлен удаленный доступ;

– учет средств удаленного доступа;

– учет сроков действия удаленного доступа;

– регистрацию и анализ событий удаленного доступа;

– проверку соблюдения установленных ограничений;

– выявление несанкционированных попыток удаленного доступа;

– пересмотр актуальности предоставленного удаленного доступа.

8.3 По результатам контроля могут приниматься решения:

– о сохранении удаленного доступа;
– об изменении параметров удаленного доступа;
– о временном ограничении удаленного доступа;
– о прекращении удаленного доступа;
– о проведении проверки или служебного разбирательства.

9. ПРИОСТАНОВЛЕНИЕ И ПРЕКРАЩЕНИЕ УДАЛЕННОГО ДОСТУПА

9.1 Удаленный доступ подлежит приостановлению или прекращению в случаях:
– отсутствия или прекращения служебной необходимости;
– окончания срока действия удаленного доступа;
– увольнения работника Учреждения, которому был предоставлен удаленный доступ;
– прекращения договора, контракта или соглашения с подрядной организацией;
– нарушения требований настоящего Порядка удаленного доступа;
– возникновения инцидента ИБ;
– компрометации аутентификационной информации;
– выявления угроз безопасности информации, связанных с удаленным доступом.

9.2 При прекращении удаленного доступа должны быть:
– заблокированы или удалены соответствующие учетные записи;
– отозваны права удаленного доступа;
– аннулированы или изменены аутентификационные данные;
– зафиксирован факт прекращения удаленного доступа.

10. ПРАВА, ОБЯЗАННОСТИ И ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЕЙ

10.1 Пользователь, которому предоставлен удаленный доступ, обязан:
– использовать удаленный доступ только в служебных целях;
– соблюдать требования локальных нормативных актов Учреждения;
– не допускать подключения к информационным системам Учреждения посторонних лиц;
– обеспечивать защиту используемого средства удаленного доступа;
– незамедлительно сообщать о признаках компрометации средства доступа, аутентификационной информации и иных инцидентах.

10.2 Пользователю запрещается:
– передавать средство удаленного доступа и учетные данные другим лицам;
– использовать несанкционированные программы удаленного доступа;
– отключать или изменять средства защиты информации;
– использовать удаленный доступ за пределами согласованных условий.

10.3 Лица, нарушившие требования настоящего Порядка удаленного доступа, несут ответственность в соответствии с законодательством Российской Федерации, локальными нормативно-правовыми актами Учреждения и условиями заключенных договоров.

11. ПОРЯДОК ПЕРЕСМОТРА

11.1 Настоящий Порядок удаленного доступа подлежит пересмотру:
– при изменении законодательства Российской Федерации и обязательных требований в области защиты информации;
– при изменении архитектуры, состава и условий функционирования информационных систем Учреждения;
– при изменении применяемых средств удаленного доступа;
– по результатам контроля, проверок, аудитов и расследований инцидентов информационной безопасности.

11.2 Плановый пересмотр настоящего Порядка удаленного доступа осуществляется не реже одного раза в три года.

11.3 Подготовку предложений по изменению настоящего Порядка удаленного доступа организуют работники, ответственные за ИБ.

Приложение № 1
к Порядку удаленного доступа пользователей к
информационным системам ГАПОУ СО «БПТ» и
содержащейся в них информации

Форма заявки на предоставление удаленного доступа к информационной системе

ЗАЯВКА
на предоставление удаленного доступа к информационной системе

1. Сведения о работнике	
Фамилия, имя, отчество работника	
Должность	
Структурное подразделение	
Номер телефона, адрес электронной почты	
2. Сведения об информационной системе (ИС) и удаленном доступе	
Наименование ИС (нужное отметить)	□ ФИС ФРДО □ ФИС «ГИА и Приема» □ ГИС «Профилактика» □ АИС «Зачисление ПОО» □ АС «Бухгалтерия и кадры» □ АС «Студенты» □ ЕТД
Состав информации, удаленный доступ к которой предоставляется	
Требуемый объем прав доступа	
Вид удаленного доступа	□ удаленный пользовательский доступ □ удаленный доступ с расширенными правами □ удаленный привилегированный доступ □ иной вид удаленного доступа (указать вид)
Основание предоставление удаленного доступа	
Цель предоставления удаленного доступа	
Срок предоставления удаленного доступа	с «__» _____ 202_ г. по «__»_____ 202_ г.
Периодичность использования удаленного доступа (нужно отметить)	□ ежедневно □ по рабочим дням □ по мере необходимости □ иное:
Режим использования удаленного доступа (нужное отметить)	□ в рабочее время □ вне рабочего времени □ круглосуточно □ по согласованному графику (указать режим использования): с __ ч. __ мин. по __ ч. __ мин.

3. Сведения о средстве удаленного доступа и систем защиты	
Средство удаленного доступа	
Инвентарный номер ПЭВМ	
Адрес места использования устройства	
Антивирусное ПО (указать реквизиты сертификата ФСТЭК России)	
СЗИ (указать реквизиты сертификата ФСТЭК России)	
Средство защиты каналов связи (указать реквизиты сертификата ФСТЭК России)	
4. Дополнительные сведения	
Дополнительные права доступа	

Фамилия, имя, отчество работника _____ _____

(личная подпись, дата) (расшифровка подписи)

Работник, ответственный за информационную безопасность _____ _____

(личная подпись, дата) (расшифровка подписи)

Директор ГАПОУ СО «БПТ»: _____ _____

(личная подпись, дата) (расшифровка подписи)

Приложение № 4
к Внутреннему стандарту по защите информации

Порядок предоставления пользователям доступа из информационных систем в телекоммуникационную сеть «Интернет» и контроля ее использования

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Порядок предоставления пользователям доступа из информационных систем к телекоммуникационной сети «Интернет» (далее – Порядок) и контроля ее использования в ГАПОУ СО «Балаковский политехнический техникум» (далее – Учреждение) определяет:

– цели, принципы и условия предоставления пользователям ИС Учреждения доступа в сеть «Интернет»;

– уровни доступа пользователей ИС Учреждения в телекоммуникационную сеть «Интернет» (далее – сеть «Интернет»);

– порядок предоставления, изменения, приостановления и прекращения доступа пользователей ИС Учреждения в сеть «Интернет»;

– требования к использованию сети «Интернет» из ИС Учреждения;

– порядок контроля использования сети «Интернет» из ИС Учреждения;

– права, обязанности и ответственность работников Учреждения при использовании сети «Интернет» из ИС Учреждения;

– порядок пересмотра настоящего Порядка.

1.2 Настоящий Порядок является неотъемлемой частью организационных мер по обеспечению информационной безопасности на объектах информатизации Учреждения и входит в состав общих организационно-распорядительных мер, реализующихся в рамках Политики информационной безопасности Учреждения.

1.3 Настоящий Порядок разработан в целях установления единого подхода к предоставлению пользователям ИС Учреждения доступа в сеть «Интернет» и обеспечения контроля ее использования в интересах защиты информации, обрабатываемой в ИС Учреждения.

1.4 Предоставление пользователям ИС Учреждения доступа в сеть «Интернет» осуществляется с соблюдением следующих принципов:

– законности;

– обоснованности и служебной необходимости;

– минимально необходимого объема доступа;

– персональной ответственности пользователя ИС Учреждения;

– обязательности применения организационных и технических мер защиты информации;

– разграничения прав доступа;

– контролируемости и подотчетности использования сети «Интернет».

1.5 Доступ пользователей ИС Учреждения в сеть «Интернет» предоставляется исключительно для исполнения должностных обязанностей и/или решения задач, связанных с функционированием ИС Учреждения.

1.6 Использование сети «Интернет» из ИС Учреждения в личных целях не допускается, за исключением случаев, прямо установленных локальными нормативными актами Учреждения.

1.7 Настоящий Порядок является обязательным для исполнения всеми работниками Учреждения, которым предоставлен доступ к ИС Учреждения и/или в сеть «Интернет» из ИС Учреждения.

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1 Требования настоящего Порядка распространяются на:

– федеральные, государственные и объектовые ИС Учреждения;

– автоматизированные рабочие места, серверы, виртуальные машины, иные конечные устройства и программные средства, входящие в состав ИС Учреждения и обеспечивающие возможность доступа в сеть «Интернет»;

– пользователей ИС Учреждения;

– работников, участвующих в предоставлении, настройке, сопровождении и контроле доступа в сеть «Интернет» из ИС Учреждения;

– работников, ответственных за ИБ.

2.2 Требования настоящего Порядка подлежат применению при:

– предоставлении нового доступа в сеть «Интернет» из ИС Учреждения;

– изменении уровня доступа в сеть «Интернет»;

– временном расширении доступа в сеть «Интернет»;

– приостановлении и прекращении доступа в сеть «Интернет» из ИС Учреждения;

– осуществлении контроля использования сети «Интернет» из ИС Учреждения;

– проведении проверок соблюдения требований информационной безопасности при использовании сети «Интернет» из ИС Учреждения.

2.3 Настоящий Порядок не регулирует порядок предоставления пользователям удаленного доступа к ИС Учреждения, который определяется отдельными локальным нормативно-правовыми актами Учреждения.

3. КАТЕГОРИИ ИС И ОБЩИЙ РЕЖИМ ДОСТУПА

3.1 Для целей настоящего Порядка в Учреждении устанавливаются следующие категории ИС Учреждения:

– федеральные ИС, доступ к которым предоставляется из ИС Учреждения;

– государственные ИС, доступ к которым предоставляется из ИС Учреждения;

– региональные ИС, доступ к которым предоставляется из ИС Учреждения;

– объектовые ИС Учреждения.

3.2 К федеральным, государственным и региональным ИС для целей настоящего Порядка относятся ИС, используемые для взаимодействия с федеральными государственными информационными системами, государственными информационными системами, региональными информационными системами и иными информационными ресурсами публично-правовых образований, доступ к которым осуществляется в установленном порядке.

3.3 К объектовым ИС Учреждения относятся ИС Учреждения, функционирующие в пределах инфраструктуры Учреждения и не относящиеся к федеральным и государственным ИС Учреждения.

3.4 Для федеральных, государственных и региональных ИС, доступ к которым предоставляется из ИС Учреждения устанавливается ограничительный режим доступа в сеть «Интернет», предусматривающий:

– предоставление доступа только в объеме, необходимом для функционирования ИС Учреждения и исполнения трудовых (должностных) обязанностей работников Учреждения;

– использование заранее определенных ресурсов сети «Интернет», сетевых адресов, доменных имен, сервисов, портов и протоколов;

– запрет свободного пользовательского доступа в сеть «Интернет», если иное не установлено решением Учреждения и не обусловлено служебной необходимостью;

– обязательное применение организационных и технических мер защиты информации, установленных в Учреждении.

3.5 Для объектовых ИС Учреждения допускается регламентированный доступ пользователей в сеть «Интернет» в объеме, необходимом для исполнения трудовых (должностных) обязанностей, с соблюдением требований настоящего Порядка, а также организационных и технических мер защиты информации, установленных локальными нормативно-правовыми актами Учреждения в области ИБ.

3.6 Для серверов, системных учетных записей, технологических учетных записей, а также привилегированных учетных записей доступ в сеть «Интернет» предоставляется только при наличии документально подтвержденной служебной необходимости и в объеме, необходимом для функционирования ИС Учреждения.

4. УРОВНИ ДОСТУПА К СЕТИ «ИНТЕРНЕТ»

4.1 В Учреждении устанавливаются следующие уровни доступа пользователей ИС Учреждения в сеть «Интернет»:

– Уровень 0 — доступ отсутствует;

– Уровень 1 — ограниченный служебный веб-доступ;

– Уровень 2 — расширенный служебный веб-доступ;

– Уровень 3 — расширенный временный доступ;

– Уровень 4 — расширенный постоянный доступ.

4.2 Уровень 0 — доступ отсутствует.

Данный уровень устанавливается по умолчанию для пользователей ИС Учреждения, если доступ в сеть «Интернет» не требуется для исполнения должностных обязанностей или функционирования ИС Учреждения.

4.3 Уровень 1 — ограниченный служебный веб-доступ.

Данный уровень предусматривает доступ к ограниченному перечню ресурсов сети «Интернет», необходимых для исполнения должностных обязанностей, посредством браузера и (или) иных утвержденных программных средств, с применением фильтрации и контроля трафика.

При уровне 1 допускается доступ только к заранее разрешенным ресурсам сети «Интернет» либо к ресурсам разрешенных категорий в соответствии с настройками средств защиты информации Учреждения.

4.4 Уровень 2 — расширенный служебный веб-доступ.

Данный уровень предусматривает служебный веб-доступ в сеть «Интернет» в более широком объеме по сравнению с уровнем 1, необходимый для исполнения должностных обязанностей, при обязательном применении средств фильтрации, журналирования и иных мер защиты информации.

При уровне 2 допускается доступ к ресурсам сети «Интернет», необходимым для выполнения служебных задач, за исключением запрещенных категорий ресурсов, сервисов и направлений взаимодействия, установленных в Учреждении.

4.5 Уровень 3 — расширенный временный доступ.

Данный уровень предусматривает предоставление пользователю ИС Учреждения на ограниченный срок расширенного доступа в сеть «Интернет» при наличии документально подтвержденной служебной необходимости.

Расширенный временный доступ предоставляется на срок, указанный в заявке, и подлежит обязательному прекращению по истечении установленного срока либо при отпадении необходимости в нем.

4.6 Уровень 4 — расширенный постоянный доступ.

Данный уровень предусматривает предоставление пользователю ИС Учреждения постоянного расширенного доступа в сеть «Интернет» при наличии устойчивой служебной необходимости, подтвержденной руководителем соответствующего структурного подразделения Учреждения и согласованной в установленном порядке.

Расширенный постоянный доступ устанавливается только в тех случаях, когда исполнение должностных обязанностей невозможно или существенно затруднено при использовании уровней 1 или 2.

4.7 Конкретный уровень доступа в сеть «Интернет» определяется с учетом:

– категории ИС Учреждения;

– характера должностных обязанностей работника Учреждения;

– необходимости использования внешних ресурсов сети «Интернет»;

– состава обрабатываемой в ИС Учреждения информации;

– требований локальных нормативных актов Учреждения в области информационной безопасности.

5. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОСТУПА К СЕТИ «ИНТЕРНЕТ»

5.1 Основанием для предоставления пользователю ИС Учреждения доступа в сеть «Интернет» является служебная необходимость.

5.2 Доступ в сеть «Интернет» предоставляется на основании заявки, оформляемой руководителем структурного подразделения Учреждения, в котором работает пользователь ИС Учреждения, либо иным уполномоченным должностным лицом Учреждения.

5.3 В заявке на предоставление доступа в сеть «Интернет» указываются:

– фамилия, имя, отчество пользователя ИС Учреждения;

– должность пользователя ИС Учреждения;

– наименование структурного подразделения Учреждения;

– наименование ИС Учреждения;

– сведения о рабочем месте (устройстве), с которого предполагается доступ в сеть «Интернет»;

– запрашиваемый уровень доступа;

– обоснование необходимости предоставления доступа;

– предполагаемый срок предоставления доступа, если доступ требуется временно;

– перечень ресурсов сети «Интернет», если требуется предоставление доступа по ограниченному перечню ресурсов.

5.4 Заявка на предоставление доступа в сеть «Интернет» подлежит согласованию:

–руководителем структурного подразделения Учреждения, в котором работает пользователь ИС Учреждения;

– работником, ответственным за информационную безопасность, в пределах установленной компетенции;

– при необходимости – работником Учреждения, осуществляющим сопровождение соответствующей ИС Учреждения.

5.5 По результатам согласования заявки принимается решение о:

– предоставлении доступа в сеть «Интернет»;

– предоставлении доступа в сеть «Интернет» с ограничениями;

– отказе в предоставлении доступа в сеть «Интернет».

5.6 При предоставлении доступа в сеть «Интернет» пользователю ИС Учреждения:

– устанавливается соответствующий уровень доступа;

– определяются ограничения по ресурсам, сервисам, протоколам, адресам и иным параметрам доступа;

– при необходимости устанавливается срок действия доступа;

– обеспечивается настройка средств защиты информации и средств контроля использования сети «Интернет».

5.7 Доступ в сеть «Интернет» может предоставляться:

– на постоянной основе;

– на временной основе;

– однократно для выполнения конкретной служебной задачи.

5.8 Изменение уровня доступа, расширение доступа, ограничение доступа, приостановление доступа и прекращение доступа осуществляются в порядке, аналогичном порядку первоначального предоставления доступа, если иное не установлено настоящим Порядком.

5.9 Доступ в сеть «Интернет» подлежит прекращению в случаях:

– увольнения работника Учреждения;

– перевода работника Учреждения на иную должность, не требующую предоставленного уровня доступа;

– отпадения служебной необходимости;

– истечения срока временного доступа;

– выявления нарушений требований настоящего Порядка;

– возникновения инцидента ИБ;

– принятия соответствующего решения директором Учреждения.

6. ТРЕБОВАНИЯ К ИСПОЛЬЗОВАНИЮ СЕТИ «ИНТЕРНЕТ» ИЗ ИС

6.1 Доступ в сеть «Интернет» из ИС Учреждения осуществляется только через контролируемую информационно-телекоммуникационную инфраструктуру Учреждения и с использованием штатных средств доступа, программного обеспечения, средств антивирусной защиты и средств защиты информации, разрешенных к применению в Учреждении.

6.2 При использовании сети «Интернет» из ИС Учреждения должны применяться предусмотренные в Учреждении организационные и технические меры защиты информации, включая:

– средства защиты информации;

– средства антивирусной защиты;

– механизмы идентификации и аутентификации;

– механизмы двухфакторной аутентификации в случаях, предусмотренных локальными нормативно-правовыми актами Учреждения в области ИБ;

– средства фильтрации и контроля сетевого трафика;

– средства журналирования событий безопасности;

– механизмы разграничения прав доступа.

6.3 Использование сети «Интернет» из ИС Учреждения допускается только с ПЭВМ и устройств, учтенных в установленном в Учреждении порядке и соответствующих утвержденным требованиям к конфигурации и защите.

6.4 Пользователям ИС Учреждения запрещается:

– отключать, изменять или иным образом вмешиваться в работу средств защиты информации;

– использовать несанкционированное ПО;

– устанавливать программное обеспечение, расширения браузеров, плагины, агенты удаленного доступа и иные программные компоненты без предварительного согласования с работником, ответственным за ИБ;

– использовать средства обхода сетевых ограничений;

– использовать личные учетные записи внешних сервисов, не предназначенных для служебной деятельности, если иное не установлено локальными нормативными актами Учреждения;

– передавать в сеть «Интернет» информацию, доступ к которой ограничен, с нарушением требований локальных нормативных актов Учреждения;

– использовать личные точки доступа, внешние каналы связи и иные неконтролируемые способы подключения к сети «Интернет»;

– предоставлять третьим лицам возможность использования своего рабочего места и/или своих учетных данных для выхода в сеть «Интернет» из ИС Учреждения.

6.5 Для федеральных, государственных и региональные ИС Учреждения дополнительно устанавливаются следующие требования:

–доступ в сеть «Интернет» предоставляется только в пределах служебной необходимости;

–приоритетным является предоставление доступа по ограниченному перечню ресурсов;

–не допускается использование сервисов и ресурсов сети «Интернет», не обусловленных задачами соответствующей ИС Учреждения и должностными обязанностями пользователя ИС Учреждения;

–взаимодействие с внешними ресурсами сети «Интернет» осуществляется через предусмотренные в Учреждении средства защиты информации и средства контроля.

6.6 Для объектовых ИС Учреждения доступ в сеть «Интернет» осуществляется в соответствии с установленным уровнем доступа, с учетом задач соответствующей ИС Учреждения и при обязательном соблюдении требований информационной безопасности, действующих в Учреждении.

7. КОНТРОЛЬ ИСПОЛЬЗОВАНИЯ СЕТИ «ИНТЕРНЕТ»

7.1 Контроль использования сети «Интернет» из ИС Учреждения осуществляется работниками, ответственными за ИБ.

7.2 Контроль использования сети «Интернет» включает:

– учет пользователей ИС Учреждения, которым предоставлен доступ в сеть «Интернет»;

– учет рабочих мест и устройств, с которых предоставлен доступ в сеть «Интернет»;

– учет уровней доступа в сеть «Интернет»;

– учет перечней разрешенных ресурсов сети «Интернет»;

– регистрацию и анализ событий, связанных с использованием сети «Интернет»;

– выявление нарушений требований настоящего Порядка;

– контроль актуальности предоставленных прав доступа;

– проведение проверок соблюдения требований информационной безопасности при использовании сети «Интернет».

7.3 Подлежат регистрации и анализу, в том числе, следующие события:

– предоставление, изменение, приостановление и прекращение доступа в сеть «Интернет»;

– успешные и неуспешные попытки обращения к ресурсам сети «Интернет»;

– попытки доступа к запрещенным ресурсам и сервисам;

– попытки обхода установленных ограничений;

– факты использования несанкционированного программного обеспечения;

– события, указывающие на возможный инцидент информационной безопасности;

– изменения конфигурации средств доступа в сеть «Интернет» и средств защиты информации.

7.4 Журналы событий, связанные с использованием сети «Интернет», подлежат хранению и защите в порядке, установленном в Учреждении.

7.5 По результатам контроля использования сети «Интернет» могут приниматься решения о:

– сохранении ранее предоставленного уровня доступа;

– изменении уровня доступа;

– введении дополнительных ограничений;

– приостановлении или прекращении доступа;

– проведении служебной проверки;

– применении мер ответственности в соответствии с законодательством Российской Федерации и локальными нормативными актами Учреждения.

8. ПРАВА И ОБЯЗАННОСТИ

8.1 Пользователь ИС Учреждения имеет право:

– использовать предоставленный доступ в сеть «Интернет» в пределах установленного уровня доступа и для исполнения должностных обязанностей;

– обращаться с заявкой на предоставление, изменение или расширение доступа в сеть «Интернет» в установленном порядке;

– получать информацию о действующих ограничениях и правилах использования сети «Интернет» из ИС Учреждения.

8.2 Пользователь ИС Учреждения обязан:

– использовать сеть «Интернет» только для исполнения должностных обязанностей;

– соблюдать требования настоящего Порядка и иных локальных нормативных актов Учреждения в области информационной безопасности;

– обеспечивать сохранность своих учетных данных;

– незамедлительно сообщать работникам, ответственным за ИБ о выявленных признаках инцидента ИБ, попытках несанкционированного доступа, сбоях средств защиты информации и иных событиях, способных повлиять на безопасность ИС Учреждения;

– выполнять законные требования работников, ответственных за ИБ.

8.3 Работники, ответственные за ИБ в пределах установленной компетенции:

– организует предоставление, изменение, приостановление и прекращение доступа пользователей ИС Учреждения в сеть «Интернет»;

– обеспечивает контроль использования сети «Интернет» из ИС Учреждения;

– участвует в согласовании заявок на предоставление доступа в сеть «Интернет»;

– определяет необходимые ограничения и дополнительные меры защиты информации;

– организует анализ журналов событий и материалов контроля;

– инициирует проведение проверок при выявлении нарушений и признаков инцидентов информационной безопасности;

– подготавливает предложения по совершенствованию порядка предоставления доступа в сеть «Интернет» и контроля ее использования.

8.4 Работники, ответственные за ИБ:

– организуют выполнение требований настоящего Порядка;

– принимают решения в пределах своей компетенции о введении дополнительных ограничений, приостановлении доступа и проведении проверок;

– докладывают директору Учреждения о выявленных нарушениях и значимых инцидентах информационной безопасности.

– участвуют в рассмотрении заявок на предоставление доступа в сеть «Интернет»;

– осуществляют контроль соблюдения требований настоящего Порядка;

– проводят анализ событий безопасности;

– подготавливают предложения по изменению уровней доступа и перечней разрешенных ресурсов сети «Интернет».

9. ОТВЕТСТВЕННОСТЬ

9.1 Работники Учреждения несут ответственность за нарушение требований настоящего Порядка в соответствии с законодательством Российской Федерации, трудовым законодательством Российской Федерации, локальными нормативными актами Учреждения и условиями трудовых договоров.

9.2 Пользователь ИС Учреждения несет персональную ответственность за:

– использование предоставленного доступа в сеть «Интернет» не по назначению;

– несоблюдение установленных ограничений;

– передачу учетных данных другим лицам;

– совершение действий, повлекших нарушение требований информационной безопасности;

– сокрытие информации о событиях, имеющих признаки инцидента информационной безопасности.

9.3 Руководители структурных подразделений Учреждения несут ответственность за обоснованность заявок на предоставление работникам Учреждения доступа в сеть «Интернет» и за контроль соблюдения работниками Учреждения требований настоящего Порядка в пределах своей компетенции.

9.4 Работники, ответственные за ИБ, несут ответственность за ненадлежащее исполнение обязанностей по организации и контролю использования сети «Интернет» из ИС Учреждения в пределах своей компетенции.

9.5 В случае выявления нарушения требований настоящего Порядка к работнику Учреждения могут применяться меры дисциплинарного воздействия, а также иные меры, предусмотренные законодательством Российской Федерации и локальными нормативными актами Учреждения.

10. ПОРЯДОК ПЕРЕСМОТРА

10.1 Настоящий Порядок подлежит пересмотру:

– при изменении законодательства Российской Федерации, нормативных правовых актов Российской Федерации и обязательных требований в области защиты информации;

– при изменении локальных нормативно-правовых актов Учреждения в области ИБ;

– при изменении состава, структуры, архитектуры или условий функционирования ИС Учреждения;

– при изменении применяемых в Учреждении средств защиты информации и средств доступа в сеть «Интернет»;

– по результатам проверок, аудитов, оценки соответствия, служебных проверок и расследования инцидентов информационной безопасности;

– при выявлении необходимости актуализации настоящего Порядка по решению директора Учреждения.

10.2 Плановый пересмотр настоящего Порядка осуществляется не реже одного раза в три года.

10.3 Подготовку предложений по внесению изменений в настоящий Порядок организуют работники, ответственные за ИБ.

Приложение № 5
к Внутреннему стандарту по защите информации

Порядок повышения уровня знаний и информированности пользователей по вопросам защиты информации в ГАПОУ СО «БПТ»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящий Порядок повышения уровня знаний и информированности пользователей по вопросам защиты информации (далее – Порядок) определяет цели, формы, периодичность и порядок организации мероприятий по повышению уровня знаний и информированности пользователей информационных систем ГАПОУ СО «БПТ» (далее – Учреждение) по вопросам защиты информации.

1.2 Требования настоящего Порядка распространяются на пользователей информационных систем Учреждения, включая работников Учреждения, которым предоставлен доступ к информационным системам Учреждения и содержащейся в них информации.

1.3 Организация мероприятий по повышению уровня знаний и информированности пользователей по вопросам защиты информации осуществляется работниками, ответственными за ИБ.

2. ЦЕЛИ ПОВЫШЕНИЯ УРОВНЯ ЗНАНИЙ И ИНФОРМИРОВАННОСТИ ПОЛЬЗОВАТЕЛЕЙ

2.1 Повышение уровня знаний и информированности пользователей осуществляется в целях:

– формирования у пользователей устойчивых знаний по вопросам защиты информации;

– снижения риска нарушений требований локальных нормативных актов Учреждения в области защиты информации;

– формирования навыков безопасной работы в информационных системах Учреждения;

– повышения устойчивости пользователей к методам социальной инженерии;

– обеспечения правильных действий пользователей при выявлении событий и инцидентов информационной безопасности.

3. ОСНОВНЫЕ ФОРМЫ МЕРОПРИЯТИЙ

3.1 Повышение уровня знаний и информированности пользователей по вопросам защиты информации осуществляется в следующих формах:

– доведение до пользователей информационных материалов по вопросам защиты информации;

– проведение инструктажей, лекций, семинаров и иных обучающих мероприятий;

– проведение имитационных рассылок электронных писем на служебные адреса электронной почты и иные служебные средства коммуникации;

– проведение тренировок по практической отработке действий, предусмотренных локальными нормативными актами Учреждения в области защиты информации.

3.2 В качестве информационных материалов могут использоваться памятки, уведомления, презентации, методические материалы и иные материалы по актуальным вопросам защиты информации.

4. ТЕМАТИКА МЕРОПРИЯТИЙ

4.1 Мероприятия по повышению уровня знаний и информированности пользователей должны включать вопросы:

– соблюдения Политики информационной безопасности Учреждения;

– соблюдения порядка предоставления доступа к информационным системам Учреждения и содержащейся в них информации;

– соблюдения порядка удаленного доступа к информационным системам Учреждения и содержащейся в них информации;

– соблюдения порядка предоставления пользователям доступа из информационных систем в сеть «Интернет» и контроля ее использования;

– правил использования аутентификационной информации, средств двухфакторной аутентификации, средств защиты информации и антивирусной защиты;

– признаков фишинга, социальной инженерии и иных распространенных угроз безопасности информации;

– порядка действий при выявлении подозрительных событий, нарушений и компьютерных инцидентов;

– правил обработки и защиты информации ограниченного доступа.

4.2 Тематика мероприятий может уточняться работниками, ответственными за ИБ с учетом используемых в Учреждении информационных систем, состава локальных нормативных актов и актуальных угроз безопасности информации.

5. ПЕРИОДИЧНОСТЬ И ОЦЕНКА УРОВНЯ ЗНАНИЙ

5.1 Мероприятия по повышению уровня знаний и информированности пользователей проводятся на плановой и внеплановой основе.

5.2 Плановые мероприятия организуются в сроки, определяемые Учреждением.

5.3 Оценка уровня знаний пользователей по вопросам защиты информации проводится:

– не реже одного раза в три года;

– после компьютерного инцидента, произошедшего в Учреждении.

5.4 Оценка уровня знаний может проводиться в форме тестирования, опроса, собеседования, анализа результатов тренировок и имитационных рассылок либо в иной форме, определенной Учреждением.

5.5 Для пользователей, показавших недостаточный уровень знаний по вопросам защиты информации, организуется повторное прохождение обучающих мероприятий.

6. ДОКУМЕНТИРОВАНИЕ МЕРОПРИЯТИЙ

6.1 Факт проведения мероприятий по повышению уровня знаний и информированности пользователей, а также результаты оценки уровня знаний подлежат учету.

6.2 Учет проведения мероприятий и результатов оценки знаний осуществляется в журнале учета обучения пользователей по вопросам защиты информации.

6.3 Форма журнала учета обучения пользователей по вопросам защиты информации приведена в Приложении № 1 к настоящему Порядку.

6.4 В журнале учета обучения пользователей по вопросам защиты информации рекомендуется отражать:

– дату проведения мероприятия;

– форму проведения мероприятия;

– тему мероприятия;

– фамилии и инициалы пользователей, прошедших обучение;

– результаты проверки знаний при ее проведении;

– сведения о повторном обучении при необходимости.

7. ОТВЕТСТВЕННОСТЬ

7.1 Пользователи обязаны участвовать в мероприятиях по повышению уровня знаний и информированности по вопросам защиты информации и выполнять требования локальных нормативно-правовых актов Учреждения в области защиты информации.

7.2 Работники, ответственные за ИБ организуют проведение мероприятий, учет их результатов и при необходимости подготовку предложений по повторному обучению пользователей.

7.3 Руководители структурных подразделений Учреждения обеспечивают участие подчиненных работников в мероприятиях, проводимых в соответствии с настоящим Порядком.

8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

8.1 Настоящий Порядок вступает в силу со дня его утверждения.

8.2 Пересмотр настоящего Порядка осуществляется при изменении требований законодательства Российской Федерации, требований ФСТЭК России, локальных нормативных актов Учреждения в области защиты информации, а также при необходимости актуализации тематики и форм обучения.

Приложение № 1
к Порядку повышения уровня знаний и информированности
пользователей по вопросам защиты информации в ГАПОУ СО «БПТ»

Форма журнала учета обучения пользователей по вопросам защиты информации

Государственное автономное профессиональное образовательное учреждение Саратовской области «Балаковский политехнический техникум»

ЖУРНАЛ
учета обучения пользователей по вопросам защиты информации

Начат: «___» _____ 20 ___ г.
Окончен: «___» _____ 20 ___ г.

На _____ листах
Срок хранения: _____ лет

г. Балаково

№ п/п	Дата проведения	Форма проведения	Тема мероприятия	ФИО работников, проходящих обучение	Подписи	ФИО ответственного лица	Подпись	Сведения о необходимости повторного обучения

Приложение № 6
к Внутреннему стандарту по защите информации

Порядок выявления, оценки и устранения уязвимостей информационных систем

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящий Порядок выявления, оценки и устранения уязвимостей информационных систем (далее – Порядок) определяет цели, условия и порядок организации в ГАПОУ СО «БПТ» (далее – Учреждение) работ по выявлению уязвимостей информационных систем Учреждения, оценке их критичности, определению методов и приоритетов устранения, применению компенсирующих мер и контролю устранения уязвимостей.

1.2 Настоящий Порядок разработан в целях выполнения требований локальных нормативных актов Учреждения в области защиты информации и требований ФСТЭК России к управлению уязвимостями.

1.3 Требования настоящего Порядка распространяются на федеральные, государственные, объектовые и иные информационные системы Учреждения, а также на программные, программно-аппаратные средства и конечные устройства, входящие в состав указанных информационных систем.

1.4 Организация работ по выявлению, оценке и устранению уязвимостей осуществляется работниками, ответственными за ИБ во взаимодействии с работниками Учреждения, обеспечивающими эксплуатацию информационных систем.

2. ЦЕЛИ УПРАВЛЕНИЯ УЯЗВИМОСТЯМИ

2.1 Управление уязвимостями осуществляется в целях:

– своевременного выявления уязвимостей информационных систем Учреждения;

– определения критичности выявленных уязвимостей;

– минимизации риска использования уязвимостей нарушителем;

– своевременного устранения уязвимостей либо исключения возможности их использования за счет компенсирующих мер;

– контроля состояния защищенности информационных систем Учреждения.

2.2 Выявление уязвимостей может осуществляться автоматизированным и (или) ручным способом с последующей экспертной оценкой возможности их использования нарушителем.

3. ОСНОВНЫЕ МЕРОПРИЯТИЯ ПО УПРАВЛЕНИЮ УЯЗВИМОСТЯМИ

3.1 Управление уязвимостями включает:

– выявление уязвимостей информационных систем Учреждения;

– оценку критичности выявленных уязвимостей;

– определение методов и приоритетов устранения уязвимостей;

– устранение уязвимостей;

– применение компенсирующих мер в случае невозможности немедленного устранения уязвимости;

– контроль устранения уязвимостей.

4. ПОРЯДОК ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ

4.1 Выявление уязвимостей осуществляется:

– в плановом порядке;

– при вводе в эксплуатацию новых программных и программно-аппаратных средств;

– при изменении конфигурации информационной системы;

– при получении сведений об актуальных уязвимостях из доверенных источников;

– после компьютерных инцидентов;

– при проведении контроля уровня защищенности информации.

4.2 Источниками сведений об уязвимостях могут являться:

– результаты сканирования защищенности;

– результаты анализа конфигураций;

– сообщения разработчиков и производителей программных и программно-аппаратных средств;

– сведения Банка данных угроз безопасности информации ФСТЭК России;

– результаты внутренних проверок и анализа событий безопасности.

4.3 По результатам выявления уязвимости составляется акт по результатам выявления, оценки и устранения уязвимостей информационной системы, в котором обязательно фиксируются:

– дата выявления;

– наименование информационной системы Учреждения;

– программное, программно-аппаратное средство и компонент, в котором выявлена уязвимость;

– описание уязвимости;

– источник информации об уязвимости;

– предварительная оценка возможности использования уязвимости.

4.4 По фактам выявления уязвимостей, требующих комиссионного рассмотрения, проведения обследования, определения компенсирующих мер либо подтверждения устранения уязвимости, в Учреждении оформляется акт комиссии по результатам выявления, оценки и устранения уязвимостей информационной системы по форме согласно приложению № 1 к настоящему Порядку.

4.5 Необходимость создания комиссии определяется директором Учреждения.

4.6 Учет выявленных уязвимостей ведется в журнале учета уязвимостей информационных систем.

4.7 Форма журнала учета уязвимостей информационных систем представлена в приложении № 2 к настоящему Порядку.

5. ПОРЯДОК ОЦЕНКИ КРИТИЧНОСТИ УЯЗВИМОСТЕЙ

5.1 После выявления уязвимости работники, ответственные за ИБ организуют оценку ее критичности.

5.2 При оценке критичности учитываются:

– возможность использования уязвимости нарушителем;

– доступность уязвимого компонента из сети связи;

– наличие в информационной системе информации ограниченного доступа;

– возможные последствия нарушения конфиденциальности, целостности, доступности информации и нарушения функционирования информационной системы;

– наличие и эффективность уже применяемых мер защиты информации;

– наличие сведений об эксплуатации уязвимости в реальных атаках.

5.3 По результатам оценки уязвимости присваивается один из уровней опасности:

– критический;

– высокий;

– средний;

– низкий.

6. ПОРЯДОК УСТРАНЕНИЯ УЯЗВИМОСТЕЙ И ПРИМЕНЕНИЯ КОМПЕНСИРУЮЩИХ МЕР

6.1 По каждой выявленной уязвимости определяется способ реагирования:

– установка обновления;

– изменение конфигурации;

– отключение или ограничение уязвимой функции;

– ограничение сетевого доступа;

– изоляция компонента;

– усиление контроля и мониторинга;

– применение иных компенсирующих мер;

– вывод уязвимого компонента из эксплуатации.

6.2 Устранение уязвимостей либо исключение возможности их использования за счет компенсирующих мер осуществляется в следующие сроки:

– для уязвимостей критического уровня опасности — не более 24 часов;

– для уязвимостей высокого уровня опасности — не более 7 календарных дней;

– для уязвимостей среднего уровня опасности — не более 30 календарных дней;

– для уязвимостей низкого уровня опасности — не более 90 календарных дней.

6.3 Если устранение уязвимости в установленный срок невозможно, работники, ответственные за ИБ, совместно с работниками Учреждения, обеспечивающими эксплуатацию информационной системы, определяют и документируют компенсирующие меры, исключающие либо существенно снижающие возможность использования уязвимости.

6.4 До устранения уязвимости или введения компенсирующих мер при необходимости могут приниматься решения:

– о временном ограничении доступа к отдельным функциям;

– о временном отключении уязвимого компонента;

– о введении дополнительных мер мониторинга;

– о запрете удаленного доступа к уязвимому компоненту;

– о временном прекращении эксплуатации соответствующего элемента информационной системы.

7. ОСОБЕННОСТИ ВЗАИМОДЕЙСТВИЯ С УПРАВЛЕНИЕМ ОБНОВЛЕНИЯМИ

7.1 Если устранение уязвимости требует установки обновления программного или программно-аппаратного средства, такие действия выполняются с учетом локальных нормативных актов Учреждения, регулирующих управление обновлениями.

7.2 Применение обновлений, предназначенных для устранения уязвимостей, должно осуществляться с учетом рисков, связанных с установкой таких обновлений, и в сроки, обеспечивающие соблюдение требований настоящего Порядка.

8. КОНТРОЛЬ УСТРАНЕНИЯ УЯЗВИМОСТЕЙ

8.1 Контроль устранения уязвимостей осуществляется работниками, ответственными за ИБ.

8.2 Контроль включает:

– проверку соблюдения сроков устранения уязвимостей;

– проверку фактического устранения уязвимости либо результативности компенсирующих мер;

– повторную проверку уязвимого компонента;

– актуализацию сведений в журнале (реестре) уязвимостей.

8.3 Уязвимость считается устраненной после подтверждения отсутствия возможности ее использования либо после подтверждения достаточности введенных компенсирующих мер.

9. НАПРАВЛЕНИЕ СВЕДЕНИЙ ОБ УЯЗВИМОСТЯХ В ФСТЭК РОССИИ

9.1 При выявлении уязвимости информационной системы Учреждения, сведения о которой отсутствуют в Банке данных угроз безопасности информации ФСТЭК России, работники, ответственные за ИБ организуют подготовку и направление сведений о такой уязвимости в ФСТЭК России.

9.2 Направление сведений осуществляется в срок не более 5 рабочих дней с даты выявления такой уязвимости.

10. ОТВЕТСТВЕННОСТЬ

10.1 Работники Учреждения, обеспечивающие эксплуатацию информационных систем, обязаны своевременно исполнять решения по устранению уязвимостей и применению компенсирующих мер.

10.2 Пользователи информационных систем Учреждения обязаны незамедлительно сообщать работникам, ответственным за ИБ о выявленных признаках уязвимостей, нарушений безопасности информации и подозрительных событиях.

10.3 Работники, ответственные за ИБ отвечают за организацию учета уязвимостей, оценку их критичности, контроль сроков устранения и подготовку предложений по снижению рисков.

11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

11.1 Пересмотр настоящего Порядка осуществляется при изменении требований законодательства Российской Федерации, требований ФСТЭК России, локальных нормативно-правовых актов Учреждения, а также по результатам контроля, аудитов и компьютерных инцидентов.

11.2 Подготовку предложений по актуализации настоящего Порядка организуют работники, ответственные за ИБ.

Приложение № 1
к Порядок выявления, оценки и устранения
уязвимостей информационных систем

Форма акта комиссии по результатам выявления, оценки и устранения уязвимостей информационной системы

АКТ КОМИССИИ № _____
от «___» _____ 20__ г.
по результатам выявления, оценки и устранения уязвимостей информационной системы

1. Основание для проведения обследования и оформления акта
Основанием для проведения обследования информационной системы и оформления настоящего акта является: _____
☐ плановое мероприятие по выявлению уязвимостей
☐ ввод в эксплуатацию нового программного, программно-аппаратного средства
☐ изменение конфигурации информационной системы
☐ получение информации об актуальной уязвимости из доверенного источника
☐ компьютерный инцидент
☐ результат контроля уровня защищенности информации
☐ иное: _____
Реквизиты основания (приказ, служебная записка, уведомление, запись журнала, иной документ): _____
2. Сведения о комиссии
Для проведения обследования и оценки уязвимости создана комиссия в составе:
Председатель комиссии:
(должность, Ф.И.О.)
Заместитель председателя комиссии:
(должность, Ф.И.О.)
Члены комиссии:
(должность, Ф.И.О.)
(должность, Ф.И.О.)
3. Сведения об информационной системе
Наименование информационной системы:
Категория информационной системы:
☐ федеральная
☐ государственная
☐ объектовая
☐ иная: _____
Место эксплуатации: _____
Ответственный за эксплуатацию информационной системы: _____
4. Сведения о выявленной уязвимости
Дата и время выявления уязвимости: «___» _____ 20__ г.
Источник выявления уязвимости:
☐ сканирование защищенности
☐ анализ конфигурации
☐ сообщение разработчика / производителя
☐ сведения Банка данных угроз безопасности информации ФСТЭК России

☐ результат внутренней проверки
☐ результат анализа событий безопасности
☐ иное: _____
Наименование компонента, в котором выявлена уязвимость: _____
Тип компонента:
☐ программное средство
☐ программно-аппаратное средство
☐ сетевое оборудование
☐ сервер
☐ автоматизированное рабочее место
☐ иное: _____
Описание уязвимости:
_____
_____
_____
_____
Идентификатор уязвимости (при наличии): _____
Наличие сведений об уязвимости в Банке данных угроз безопасности информации ФСТЭК России:
☐ да
☐ нет
☐ не установлено
При отсутствии сведений в Банке данных угроз безопасности информации ФСТЭК России: необходимость направления сведений в ФСТЭК России:
☐ да
☐ нет

5. Проведенные мероприятия и обследования

Комиссией проведены следующие мероприятия:
☐ анализ состава и конфигурации информационной системы
☐ анализ журналов событий и событий безопасности
☐ обследование автоматизированных рабочих мест
☐ обследование серверов
☐ обследование сетевой инфраструктуры
☐ проверка версий программного обеспечения
☐ проверка наличия и актуальности обновлений
☐ проверка настроек средств защиты информации
☐ проверка возможности эксплуатации уязвимости
☐ анализ доступности уязвимого компонента из сети
☐ анализ применяемых мер защиты информации
☐ иные мероприятия: _____
Описание результатов проведенных мероприятий:
_____
_____
_____
_____

6. Оценка уязвимости

По результатам обследования комиссия установила:
6.1. Возможность использования уязвимости нарушителем

☐ подтверждена
☐ частично подтверждена
☐ не подтверждена
Описание:
_____
_____
_____
_____
6.2. Доступность уязвимого компонента
☐ из внешних сетей
☐ из внутренних сетей
☐ только локально
☐ не установлена
6.3. Возможные последствия использования уязвимости
☐ нарушение конфиденциальности информации
☐ нарушение целостности информации
☐ нарушение доступности информации
☐ нарушение функционирования информационной системы
☐ получение несанкционированного доступа
☐ повышение привилегий
☐ иное: _____
Описание возможных последствий:
_____
_____
_____
_____
6.4. Наличие и эффективность действующих мер защиты
_____
_____
_____
_____
6.5. Присвоенный уровень опасности уязвимости
☐ критический
☐ высокий
☐ средний
☐ низкий
Обоснование присвоенного уровня опасности:
_____
_____
_____
_____
7. Решение комиссии
По результатам выявления и оценки уязвимости комиссия решила:
☐ уязвимость подлежит устранению
☐ уязвимость не может быть устранена немедленно, требуется применение компенсирующих мер
☐ требуется дополнительное обследование
☐ требуется временное ограничение эксплуатации компонента
☐ требуется временное отключение компонента

☐ требуется направление сведений в ФСТЭК России

☐ иное: _____

8. Мероприятия по устранению уязвимости / компенсирующие меры

Подлежат выполнению следующие мероприятия:

№ п/п	Мероприятие	Ответственное лицо	Срок выполнения	Отметка о выполнении
1.				
2.				
3.				
4.				

При необходимости указываются компенсирующие меры:

_____

_____

_____

_____

Срок устранения уязвимости / внедрения компенсирующих мер:

_____

9. Результаты выполнения мероприятий

По состоянию на «__» _____ 20__ г. комиссией установлено:

☐ уязвимость устранена

☐ возможность использования уязвимости исключена компенсирующими мерами

☐ уязвимость устранена частично

☐ мероприятия по устранению уязвимости продолжаются

☐ требуется повторное обследование

☐ требуется принятие дополнительных мер

Описание фактически выполненных мероприятий:

_____

_____

_____

_____

Результаты повторной проверки:

_____

_____

_____

_____

10. Заключение комиссии

Комиссия пришла к следующему заключению:

☐ уязвимость устранена в полном объеме

☐ риск эксплуатации уязвимости снижен до допустимого уровня

☐ введенные компенсирующие меры признаны достаточными

☐ требуется дополнительный контроль

☐ требуется повторное рассмотрение вопроса комиссией

☐ требуется корректировка состава мер защиты информации

☐ иное: _____

Дополнительные выводы и предложения комиссии:

_____

_____
_____
_____

11. Приложения к акту

К настоящему акту прилагаются:

☐ результаты сканирования

☐ отчеты о проверке конфигурации

☐ копии уведомлений разработчиков / производителей

☐ выписки из журналов событий

☐ скриншоты / иные материалы фиксации

☐ служебные записки

☐ иные документы: _____

12. Подписи членов комиссии

Председатель комиссии

_____ /_____/

«__» _____ 20__ г.

Заместитель председателя комиссии

_____ /_____/

«__» _____ 20__ г.

Члены комиссии:

_____ /_____/

«__» _____ 20__ г.

_____ /_____/

«__» _____ 20__ г.

_____ /_____/

«__» _____ 20__ г.

_____ /_____/

«__» _____ 20__ г.

Приложение № 1
к Порядку выявления, оценки и устранения
уязвимостей информационных систем

Форма журнала учета уязвимостей информационных систем

Государственное автономное профессиональное образовательное учреждение Саратовской области «Балаковский политехнический техникум»

ЖУРНАЛ
учета уязвимостей информационных систем

Начат: «___» _____ 20 ___ г.
Окончен: «___» _____ 20 ___ г.

На _____ листах
Срок хранения: _____ лет

г. Балаково

№ п/п	Дата выявления	Информационная система	Описание уязвимости	Уровень опасности	Принятое решение	ФИО ответственного лица	Подпись	Отметка и дата устранения

Приложение № 7
к Внутреннему стандарту по защите информации

1. Порядок получения, оценки, тестирования и применения обновлений программных и программно-аппаратных средств

1.1. Порядок получения, оценки, тестирования и применения обновлений программных и программно-аппаратных средств (далее – Порядок) определяет цели, условия, последовательность и особенности организации в ГАПОУ СО «Балаковский политехнический техникум» (далее – Учреждение) работ по получению, оценке, тестированию и применению обновлений программных и программно-аппаратных средств, используемых в информационных системах Учреждения.

1.2. Настоящий Порядок разработан в целях обеспечения надлежащего уровня защиты информации, содержащейся в информационных системах Учреждения, поддержания актуального и безопасного состояния программных и программно-аппаратных средств, а также снижения риска реализации угроз безопасности информации, связанных с использованием устаревших версий программного обеспечения, микропрограммного обеспечения и иных компонентов информационных систем Учреждения.

1.3. Настоящий Порядок является локальным нормативно-правовым актом Учреждения в области ИБ и обязателен для исполнения работниками Учреждения в пределах их компетенции.

1.4. Для целей настоящего Порядка под обновлениями понимаются обновления программных и программно-аппаратных средств, в том числе:

– обновления операционных систем;

– обновления прикладного программного обеспечения;

– обновления системного программного обеспечения;

– обновления встроенного программного обеспечения, микропрограмм, прошивок;

– обновления средств защиты информации;

– обновления драйверов, библиотек, модулей и иных компонентов, влияющих на функционирование и безопасность информационных систем Учреждения.

1.5. Управление обновлениями в Учреждении осуществляется на постоянной основе и включает:

– получение сведений об обновлениях;

– оценку необходимости и допустимости их применения;

– тестирование обновлений;

– принятие решения о применении либо об отказе от применения обновлений;

– применение обновлений;

– контроль результатов применения обновлений;

– принятие компенсирующих мер в случае невозможности своевременного применения обновлений.

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1. Требования настоящего Порядка распространяются на:

– федеральные, государственные, региональные, объектовые и иные информационные системы, эксплуатируемые в Учреждении;

– автоматизированные рабочие места, серверы, сетевое оборудование, средства виртуализации, хранилища данных, иные программные и программно-аппаратные средства, входящие в состав информационных систем Учреждения;

– средства защиты информации, применяемые в информационных системах Учреждения;

– работников ответственных за ИБ;

– работников Учреждения, обеспечивающих эксплуатацию информационных систем Учреждения.

3. ЦЕЛИ И ПРИНЦИПЫ УПРАВЛЕНИЯ ОБНОВЛЕНИЯМИ

3.1. Управление обновлениями осуществляется в целях:

– своевременного устранения уязвимостей и недостатков ИБ;

– поддержания работоспособности, совместимости и устойчивости функционирования информационных систем Учреждения;

– предотвращения использования в информационных системах Учреждения устаревших и небезопасных версий программных и программно-аппаратных средств;

– недопущения негативного влияния обновлений на функционирование информационных систем Учреждения.

3.2. Получение, оценка, тестирование и применение обновлений осуществляются на основании следующих принципов:

– законности и обоснованности;

– приоритета защиты информации;

– учета влияния обновлений на функционирование информационных систем Учреждения;

– обязательности предварительной оценки обновлений;

– обязательности тестирования обновлений, кроме случаев применения срочных обновлений в особом порядке;

– дифференцированного подхода в зависимости от критичности уязвимости, значимости обновляемого компонента и возможных последствий установки обновления.

4. ОРГАНИЗАЦИЯ РАБОТ ПО УПРАВЛЕНИЮ ОБНОВЛЕНИЯМИ

4.1. Организацию работ по управлению обновлениями осуществляют работники, ответственные за ИБ во взаимодействии с работниками Учреждения, обеспечивающими эксплуатацию информационных систем Учреждения.

4.2. Работники, ответственные за ИБ:

– организуют получение информации о доступных обновлениях;

– оценивают влияние обновлений на состояние защищенности информационных систем Учреждения;

– участвуют в определении приоритетов применения обновлений;

– контролируют соблюдение сроков применения обновлений, связанных с устранением уязвимостей;

– согласовывают применение срочных обновлений;

– инициируют принятие компенсирующих мер при невозможности своевременного применения обновлений.

4.3. Работники Учреждения, обеспечивающие эксплуатацию информационных систем Учреждения:

– получают сведения об обновлениях от разработчиков, производителей и иных доверенных источников;

– проводят предварительный анализ применимости обновлений;

– организуют и проводят тестирование обновлений;

– осуществляют установку обновлений;

– контролируют технические результаты установки;

– информируют работников, ответственных за ИБ о проблемах, рисках и результатах применения обновлений.

4.4. Руководители структурных подразделений Учреждения обеспечивают выполнение мероприятий по применению обновлений в подведомственных им сегментах и компонентах информационных систем Учреждения в пределах своей компетенции.

5. ПОЛУЧЕНИЕ СВЕДЕНИЙ ОБ ОБНОВЛЕНИЯХ

5.1. Получение сведений об обновлениях осуществляется из доверенных источников, в том числе:

– официальных сайтов разработчиков и производителей;

– официальных репозиториев и сервисов обновлений;

– уведомлений разработчиков, производителей, правообладателей и поставщиков;

– технической документации;

– сведений, поступающих в рамках сопровождения программных и программно-аппаратных средств;

– сведений, полученных при выявлении и оценке уязвимостей информационных систем Учреждения.

5.2. Не допускается получение и применение обновлений из неофициальных, неподтвержденных либо недоверенных источников.

5.3. При получении сведений об обновлении должны быть установлены:

– наименование обновляемого средства;

– версия текущего и нового состояния;

– назначение обновления;

– наличие исправлений уязвимостей и ошибок;

– возможные ограничения, требования совместимости и особенности установки;

– наличие информации о рисках применения обновления.

6. ОЦЕНКА ОБНОВЛЕНИЙ

6.1. Каждое полученное обновление подлежит оценке до его применения.

6.2. В ходе оценки обновления определяется:

– относится ли обновление к средствам, применяемым в информационных системах Учреждения;

– является ли обновление обязательным для устранения уязвимости, исправления ошибки, восстановления работоспособности либо поддержания совместимости;

– затрагивает ли обновление функции защиты информации;

– может ли применение обновления повлиять на работоспособность, устойчивость, совместимость или защищенность информационной системы Учреждения;

– требуется ли предварительное резервное копирование, изменение конфигурации, остановка сервисов, уведомление пользователей или иные подготовительные мероприятия;

– необходимо ли проведение тестирования на отдельном стенде, тестовой среде либо на выделенном оборудовании.

6.3. По результатам оценки обновление относится к одной из следующих категорий:

– срочное обновление безопасности;

– плановое обновление безопасности;

– функциональное обновление;

– техническое обновление, не влияющее существенно на безопасность информации;

– обновление, применение которого временно не допускается либо откладывается до устранения выявленных рисков.

6.4. Обновления, направленные на устранение уязвимостей, оцениваются с учетом порядка выявления, оценки и устранения уязвимостей информационных систем Учреждения.

7. ТЕСТИРОВАНИЕ ОБНОВЛЕНИЙ

7.1. До применения обновлений в продуктивной среде проводится их тестирование, если это возможно с учетом архитектуры информационной системы Учреждения и характера обновления.

7.2. Тестирование обновлений проводится в целях:

– проверки корректности установки;

– проверки работоспособности обновленного средства;

– проверки совместимости обновления с иными программными и программно-аппаратными средствами;

– проверки отсутствия негативного влияния на функции защиты информации;

– оценки влияния обновления на функционирование информационной системы Учреждения.

7.3. Тестирование осуществляется:

– на тестовом стенде;

– в тестовом сегменте;

– на резервном оборудовании;

– на выделенном автоматизированном рабочем месте;

– иным способом, обеспечивающим минимизацию риска нарушения функционирования информационной системы Учреждения.

7.4. При тестировании обновлений, затрагивающих средства защиты информации, а также критически значимые компоненты информационных систем, эксплуатируемых в Учреждении, особое внимание уделяется:

– сохранению настроек безопасности;

– корректности работы механизмов идентификации, аутентификации и разграничения доступа;

– работоспособности журналирования;

– корректности работы средств антивирусной защиты, межсетевого экранирования, контроля доступа и иных средств защиты информации;

– сохранению совместимости с используемыми в Учреждении программными и программно-аппаратными средствами.

7.5. По результатам тестирования принимается одно из решений:

– обновление может быть применено в продуктивной среде;

– обновление может быть применено после выполнения дополнительных подготовительных мероприятий;

– применение обновления откладывается;

– применение обновления не допускается;

– вместо обновления должны быть применены компенсирующие меры.

8. ПРИМЕНЕНИЕ ОБНОВЛЕНИЙ

8.1. Обновления применяются по результатам их оценки и тестирования.

8.2. Перед применением обновлений при необходимости выполняются:

– резервное копирование;

– уведомление пользователей ИС, эксплуатируемых в Учреждении;

– проверка готовности к откату изменений;

– иные подготовительные мероприятия, необходимые для корректного применения обновлений.

8.3. Уведомление пользователей ИС, эксплуатируемых в Учреждении о предстоящем применении обновлений, производится не позднее чем за 30 (тридцать) минут до непосредственного начала применения обновлений.

8.4. Обновления применяются:

– планово — в рамках регламентных работ;

– внепланово — при наличии срочной необходимости;

– в экстренном порядке — при наличии критической уязвимости, признаков ее эксплуатации, возникновении инцидента ИБ, либо иных обстоятельств, требующих немедленного реагирования.

8.5. После применения обновлений обязательно должны быть проверены:

– факт корректной установки обновлений;

– работоспособность обновленного средства;

– сохранность данных и настроек обновленного средства и компонентов ИС;

– корректность взаимодействия с иными компонентами информационной системы;

– корректность работы средств защиты информации.

8.6. При обнаружении негативных последствий применения обновления принимается решение:

– об устранении выявленных проблем;

– об откате примененных обновлений;

– о временном ограничении эксплуатации обновленного компонента;

– о применении дополнительных мер защиты;

– о повторном тестировании и повторном применении обновления после устранения причин, которые привели к негативным последствиям примененных обновлений.

9. СРОЧНЫЕ ОБНОВЛЕНИЯ

9.1. Если обновление предназначено для устранения выявленной уязвимости, сроки его применения определяются с учетом уровня опасности уязвимости и рисков применения обновления.

9.2. В Учреждении устанавливаются следующие ориентиры применения обновлений, предназначенных для устранения уязвимостей:

– для критического уровня опасности — в срок не более 24 часов;

– для высокого уровня опасности — в срок не более 7 календарных дней;

– для среднего уровня опасности — в срок не более 30 календарных дней;

– для низкого уровня опасности — в срок не более 90 календарных дней.

9.3. Если применение обновления в указанные сроки невозможно без существенного риска нарушения функционирования информационной системы Учреждения, работники, ответственные за ИБ, совместно с работниками Учреждения, обеспечивающими эксплуатацию соответствующей системы, определяет и документирует компенсирующие меры, направленные на снижение риска эксплуатации уязвимости.

9.4. К компенсирующим мерам могут относиться:

– временное ограничение сетевого доступа;

– отключение уязвимой функции;

– усиление мониторинга;

– изменение конфигурации;

– временное ограничение удаленного доступа;

– изоляция уязвимого компонента;

– иные меры, исключающие или существенно затрудняющие использование уязвимости.

10. ОГРАНИЧЕНИЯ

10.1. Запрещается:

– получать обновления из недоверенных источников;

– устанавливать обновления в обход настоящего Порядка;

– применять обновления на средствах, входящих в состав информационных систем Учреждения, без оценки их влияния, за исключением срочных случаев, предусмотренных настоящим Порядком;

– самостоятельно отключать механизмы обновления, если иное не согласовано в установленном порядке;

– использовать нелицензионные, модифицированные либо неподтвержденные обновления;

– игнорировать обязательные обновления безопасности без принятия компенсирующих мер и без согласования с работниками, ответственными за ИБ.

10.2. Пользователи информационных систем Учреждения не вправе самостоятельно устанавливать обновления программных средств, если такое право прямо не предоставлено им локальными нормативно-правовыми актами Учреждения либо решением уполномоченных лиц.

11. КОНТРОЛЬ ВЫПОЛНЕНИЯ НАСТОЯЩЕГО ПОРЯДКА

11.1. Контроль выполнения настоящего Порядка осуществляется работниками, ответственными за ИБ.

11.2. Контроль включает:

– проверку своевременности получения сведений об обновлениях;

– проверку полноты оценки и тестирования обновлений;

– проверку соблюдения сроков применения обновлений;

– проверку фактического применения обязательных обновлений;

– проверку достаточности компенсирующих мер в случаях, когда обновление не было применено в установленный срок;

– анализ причин несвоевременного применения обновлений и подготовку предложений по их устранению.

12. ОТВЕТСТВЕННОСТЬ

12.1. Работники Учреждения, обеспечивающие эксплуатацию информационных систем Учреждения, несут ответственность за своевременное и надлежащее выполнение мероприятий, предусмотренных настоящим Порядком, в пределах своей компетенции.

12.2. Работники, ответственные за ИБ, несут ответственность за организацию контроля соблюдения настоящего Порядка, согласование решений по срочным обновлениям и подготовку предложений по применению компенсирующих мер.

12.3. Пользователи информационных систем Учреждения несут ответственность за нарушение установленных ограничений, связанных с самостоятельной установкой либо изменением программных и программно-аппаратных средств.

13. ПОРЯДОК ПЕРЕСМОТРА

13.1. Настоящий Порядок подлежит пересмотру:

– при изменении законодательства Российской Федерации и обязательных требований в области ИБ;

– при изменении локальных нормативно-правовых актов Учреждения;

– при изменении состава и архитектуры информационных систем Учреждения;

– при изменении применяемых средств защиты информации;

– по результатам контроля, проверок, аудитов и расследования компьютерных инцидентов;

– при необходимости уточнения сроков, этапов и способов управления обновлениями.

13.2. Плановый пересмотр настоящего Порядка осуществляется не реже одного раза в 3 года.

13.3. Подготовку предложений по актуализации настоящего Порядка организуют работники, ответственные за ИБ.

Приложение № 8
к Внутреннему стандарту по защите информации

Порядок обеспечения физической защиты информационных систем

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Порядок обеспечения физической защиты информационных систем (далее – Порядок) определяет цели, условия, требования и организацию мероприятий по обеспечению физической защиты информационных систем ГАПОУ СО «Балаковский политехнический техникум» (далее – Учреждение), а также программных и программно-аппаратных средств, машинных носителей информации и иных компонентов, входящих в состав информационных систем Учреждения.

1.2. Настоящий Порядок разработан в целях предотвращения несанкционированного физического доступа к информационным системам, эксплуатируемым в Учреждении, содержащейся в них информации, программным и программно-аппаратным средствам, машинным носителям информации, средствам защиты информации, а также в целях исключения или существенного снижения риска уничтожения, искажения, блокирования, копирования, хищения, подмены, несанкционированного подключения, демонтажа, вывода из строя либо иного неправомерного воздействия на указанные объекты.

1.3. Настоящий Порядок является локальным нормативно-правовым актом Учреждения в области защиты информации и обязателен для исполнения работниками Учреждения в пределах их компетенции.

1.4. Для целей настоящего Порядка под физической защитой понимается совокупность организационных и технических мер, направленных на контроль и ограничение физического доступа к информационным системам Учреждения, их компонентам, помещениям и зонам размещения, а также на обеспечение сохранности указанных объектов.

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1. Требования настоящего Порядка распространяются на:

– федеральные, государственные, региональные, объектовые и иные информационные системы, эксплуатируемые в Учреждении;

– автоматизированные рабочие места, серверы, сетевое оборудование, средства связи, телекоммуникационное оборудование, средства хранения данных, средства виртуализации и иные программные и программно-аппаратные средства, входящие в состав информационных систем Учреждения;

– машинные носители информации, на которых содержится информация, обрабатываемая в информационных системах Учреждения;

– средства защиты информации, применяемые в информационных системах Учреждения;

– помещения, зоны, шкафы, стойки, сейфы и иные места размещения информационных систем Учреждения и их компонентов;

– работников Учреждения, использующих информационные системы Учреждения либо обеспечивающих их эксплуатацию;

– работников, ответственных за ИБ;

– работников подрядных организаций в части, касающейся их допуска в помещения, зоны и к средствам, входящим в состав информационных систем Учреждения.

2.2. Требования настоящего Порядка применяются при:

– размещении и эксплуатации информационных систем Учреждения;

– организации доступа в помещения и зоны размещения средств обработки информации;

– эксплуатации автоматизированных рабочих мест и серверного оборудования;

– использовании, хранении, перемещении и выводе из эксплуатации машинных носителей информации и оборудования;

– проведении ремонтных, монтажных, пусконаладочных, профилактических и иных работ;

– проведении контроля соблюдения требований физической защиты.

3. ЦЕЛИ И ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ФИЗИЧЕСКОЙ ЗАЩИТЫ

3.1. Обеспечение физической защиты информационных систем Учреждения осуществляется в целях:

– предотвращения несанкционированного проникновения в помещения и зоны размещения информационных систем Учреждения;

– исключения несанкционированного физического доступа к программным и программно-аппаратным средствам;

– обеспечения сохранности машинных носителей информации, средств защиты информации и эксплуатационной документации;

– предотвращения несанкционированного подключения к средствам обработки информации и линиям связи;

– предотвращения хищения, подмены, повреждения, демонтажа и вывода из строя оборудования и носителей информации;

– поддержания непрерывности и устойчивости функционирования информационных систем Учреждения.

3.2. Физическая защита осуществляется на основании следующих принципов:

– законности;

– достаточности и соразмерности принимаемых мер;

– разграничения физического доступа;

– персональной ответственности работников Учреждения;

– минимально необходимого допуска;

– учета особенностей конкретной информационной системы, эксплуатируемой в Учреждении, состава обрабатываемой информации и условий размещения оборудования;

– обязательности контроля соблюдения установленных ограничений.

4. ОРГАНИЗАЦИЯ ФИЗИЧЕСКОЙ ЗАЩИТЫ

4.1. Организацию физической защиты информационных систем Учреждения осуществляют работники, ответственные за ИБ во взаимодействии с работниками Учреждения, обеспечивающими эксплуатацию информационных систем Учреждения, а также с иными уполномоченными работниками Учреждения.

4.2. Работники, ответственные за ИБ:

– определяет требования к физической защите помещений, зон и средств, входящих в состав информационных систем Учреждения;

– участвует в определении перечня помещений и зон, в отношении которых устанавливаются ограничения физического доступа;

– участвует в определении категорий работников, которым может быть предоставлен доступ в соответствующие помещения и зоны;

– участвует в определении мер по защите машинных носителей информации, средств защиты информации и оборудования;

– организует контроль соблюдения требований настоящего Порядка;

– инициирует принятие дополнительных мер физической защиты при выявлении нарушений, угроз или недостатков.

4.3. Работники Учреждения, обеспечивающие эксплуатацию информационных систем Учреждения:

– обеспечивают соблюдение установленных требований физической защиты;

– контролируют сохранность закрепленных за ними программных и программно-аппаратных средств;

– информируют работников, ответственных за ИБ о выявленных нарушениях, неисправностях, фактах утраты, повреждения, попытках несанкционированного доступа или иных событиях, влияющих на физическую защищенность информационных систем Учреждения.

4.4. Руководители структурных подразделений Учреждения обеспечивают соблюдение требований настоящего Порядка работниками соответствующих структурных подразделений.

5. ОБЩИЕ ТРЕБОВАНИЯ К ФИЗИЧЕСКОЙ ЗАЩИТЕ

5.1. Размещение информационных систем Учреждения, их компонентов, машинных носителей информации и средств защиты информации должно осуществляться таким образом, чтобы исключить либо существенно затруднить:

– доступ посторонних лиц;

– несанкционированное подключение к оборудованию;

– несанкционированное изъятие, замену, отключение, повреждение или демонтаж оборудования;

– визуальное ознакомление с информацией ограниченного доступа;

– несанкционированное копирование информации с машинных носителей информации;

– воздействие на оборудование и носители информации, способное привести к нарушению конфиденциальности, целостности или доступности информации.

5.2. Помещения и зоны, в которых размещаются серверы, сетевое оборудование, средства хранения данных, средства защиты информации, архивы машинных носителей информации и иные критически значимые компоненты информационных систем Учреждения, должны использоваться с учетом ограничений физического доступа.

5.3. В отношении помещений и зон, в которых размещаются средства обработки и хранения информации ограниченного доступа, должны быть определены:

–перечень лиц, имеющих право доступа;

–порядок предоставления доступа;

–порядок временного допуска иных лиц;

–порядок доступа работников подрядных организаций;

–меры контроля нахождения лиц в таких помещениях и зонах;

–меры по защите оборудования и носителей информации в нерабочее время.

5.4. Доступ в помещения и зоны размещения информационных систем Учреждения предоставляется только работникам Учреждения, которым такой доступ необходим для исполнения должностных обязанностей, а также иным лицам в установленном в Учреждении порядке.

5.5. Не допускается нахождение в помещениях и зонах размещения критически значимых компонентов информационных систем Учреждения лиц, не имеющих соответствующего допуска, без законного основания и без сопровождения, если сопровождение требуется по условиям доступа.

6. ТРЕБОВАНИЯ К ПОМЕЩЕНИЯМ, ЗОНАМ И РАЗМЕЩЕНИЮ ОБОРУДОВАНИЯ

6.1. Помещения и зоны, в которых размещаются информационные системы Учреждения либо их критически значимые компоненты, должны, по возможности, быть выделены и использоваться с учетом необходимости ограничения доступа посторонних лиц.

6.2. Программные и программно-аппаратные средства, применяемые в информационных системах Учреждения, должны размещаться:

– в помещениях или зонах, доступ в которые контролируется;

– таким образом, чтобы исключить их свободное перемещение, несанкционированное отключение либо подключение;

– с учетом требований к электропитанию, пожарной безопасности, температурному режиму и иным условиям эксплуатации, влияющим на устойчивость функционирования информационных систем Учреждения.

6.3. Серверы, сетевое оборудование, коммутационные панели, средства хранения данных, системы резервного копирования и иные критически значимые компоненты должны размещаться в условиях, исключающих свободный доступ к ним пользователей, не уполномоченных на выполнение соответствующих работ.

6.4. При размещении автоматизированных рабочих мест должны приниматься меры, исключающие:

– визуальный доступ посторонних лиц к отображаемой информации;

– несанкционированное подключение внешних устройств;

– свободный доступ к системным блокам, сетевым разъемам и машинным носителям информации, если это не требуется для исполнения должностных обязанностей.

6.5. Машинные носители информации, содержащие информацию ограниченного доступа, должны храниться в местах, исключающих свободный доступ к ним посторонних лиц.

7. ПОРЯДОК ФИЗИЧЕСКОГО ДОСТУПА

7.1. Физический доступ в помещения и зоны размещения информационных систем Учреждения предоставляется:

– на постоянной основе;

– на временной основе;

– разово для выполнения конкретных работ.

7.2. Постоянный доступ предоставляется работникам Учреждения, чьи должностные обязанности непосредственно связаны с эксплуатацией, сопровождением, администрированием либо защитой соответствующих информационных систем Учреждения.

7.3. Временный или разовый доступ предоставляется при наличии служебной необходимости, на срок, необходимый для выполнения соответствующих работ или задач.

7.4. Работники подрядных организаций допускаются в помещения и зоны размещения информационных систем Учреждения только при наличии основания, предусмотренного документами Учреждения, и в объеме, необходимом для выполнения работ или оказания услуг.

7.5. При необходимости доступ работников подрядных организаций осуществляется в сопровождении уполномоченного работника Учреждения.

7.6. Допуск работников иных организаций, посетителей и иных лиц, не являющихся работниками Учреждения, в помещения и зоны размещения информационных систем Учреждения без служебной необходимости не допускается.

8. ЗАЩИТА ОБОРУДОВАНИЯ, НОСИТЕЛЕЙ ИНФОРМАЦИИ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

8.1. Программные и программно-аппаратные средства, машинные носители информации и средства защиты информации подлежат защите от:

– несанкционированного изъятия;

– подмены;

– копирования;

– повреждения;

– уничтожения;

– несанкционированного подключения;

– несанкционированного изменения конфигурации;

– отключения и демонтажа.

8.2. 8.2. В отношении машинных носителей информации должны обеспечиваться:

– учет и контролируемое использование в случаях, предусмотренных локальными нормативными актами Учреждения;

– хранение в местах, ограничивающих физический доступ;

– защита от утраты и несанкционированного копирования;

– контролируемое перемещение между помещениями и зонами Учреждения;

– надлежащее обращение при выводе из эксплуатации, передаче, уничтожении либо обезличивании информации.

8.3. Средства защиты информации, применяемые в информационных системах Учреждения, должны размещаться и эксплуатироваться в условиях, исключающих их несанкционированное отключение, изъятие, изменение конфигурации и иное неправомерное воздействие.

8.4. Ремонт, обслуживание, замена и иные работы в отношении оборудования, входящего в состав информационных систем Учреждения, проводятся в порядке, исключающем неконтролируемый доступ к информации, машинным носителям информации и средствам защиты информации.

9. ТРЕБОВАНИЯ В НЕРАБОЧЕЕ ВРЕМЯ И ПРИ ВНЕШТАТНЫХ СИТУАЦИЯХ

9.1. В нерабочее время помещения и зоны, в которых размещаются информационные системы Учреждения и их критически значимые компоненты, должны быть приведены в состояние, исключающее свободный доступ посторонних лиц.

9.2. По окончании работы работники Учреждения обязаны:

– исключить доступ посторонних лиц к автоматизированным рабочим местам;

– обеспечить сохранность машинных носителей информации;

– при необходимости отключить, заблокировать либо перевести оборудование в безопасное состояние в соответствии с установленными правилами эксплуатации;

– обеспечить соблюдение иных требований локальных нормативных актов Учреждения.

9.3. При выявлении признаков вскрытия помещения, несанкционированного доступа, утраты оборудования, утраты машинного носителя информации, повреждения средств защиты информации либо иных событий, способных повлиять на безопасность информации, работник Учреждения обязан незамедлительно сообщить об этом работникам, ответственным за ИБ и своему непосредственному руководителю.

9.4. При возникновении аварийных, чрезвычайных и иных внештатных ситуаций должны приниматься меры, направленные на сохранность информационных систем Учреждения, машинных носителей информации и средств защиты информации, насколько это возможно в конкретных условиях.

10. ОГРАНИЧЕНИЯ

10.1. Запрещается:

– допускать в помещения и зоны размещения информационных систем Учреждения лиц, не имеющих соответствующего основания для доступа;

– оставлять без присмотра в доступных для посторонних лиц местах машинные носители информации, оборудование и документацию, содержащую сведения о конфигурации и защите информационных систем Учреждения;

– передавать ключи, пропуска, идентификаторы и иные средства доступа к помещениям и зонам другим лицам без установленного основания;

– подключать к оборудованию, входящему в состав информационных систем Учреждения, несанкционированные устройства;

– самостоятельно перемещать, разбирать, демонтировать либо заменять оборудование без соответствующего разрешения;

– оставлять автоматизированные рабочие места в состоянии, допускающем использование посторонними лицами;

– размещать оборудование и машинные носители информации в местах, не обеспечивающих требуемый уровень физической защиты.

10.2. Пользователи информационных систем Учреждения обязаны обеспечивать физическую сохранность закрепленных за ними средств и не допускать их использования посторонними лицами.

11. КОНТРОЛЬ СОБЛЮДЕНИЯ ТРЕБОВАНИЙ ФИЗИЧЕСКОЙ ЗАЩИТЫ

11.1. Контроль соблюдения требований настоящего Порядка осуществляется работниками, ответственными за ИБ.

11.2. Контроль включает:

– проверку соблюдения установленного порядка доступа в помещения и зоны размещения информационных систем Учреждения;

– проверку соблюдения требований к размещению оборудования и носителей информации;

– проверку сохранности средств защиты информации;

– проверку соблюдения запретов и ограничений, предусмотренных настоящим Порядком;

– проверку состояния физической защищенности помещений, зон и оборудования;

– подготовку предложений по устранению выявленных нарушений и недостатков.

11.3. По результатам контроля могут приниматься решения:

– о сохранении действующего порядка физической защиты;

– о введении дополнительных ограничений доступа;

– о необходимости изменения размещения оборудования;

– о принятии дополнительных организационных и технических мер;

– о проведении служебной проверки;

– о временном ограничении эксплуатации соответствующих средств или помещений.

12. ОТВЕТСТВЕННОСТЬ

12.1. Работники Учреждения несут ответственность за нарушение требований настоящего Порядка в соответствии с законодательством Российской Федерации, локальными нормативными актами Учреждения и условиями трудовых договоров.

12.2. Руководители структурных подразделений Учреждения несут ответственность за организацию соблюдения требований настоящего Порядка подчиненными работниками в пределах своей компетенции.

12.3. Работники Учреждения, обеспечивающие эксплуатацию информационных систем Учреждения, несут ответственность за сохранность закрепленных за ними средств и соблюдение требований физической защиты в пределах своей компетенции.

12.4. Работники, ответственные за ИБ несут ответственность за организацию контроля соблюдения настоящего Порядка и подготовку предложений по совершенствованию мер физической защиты.

13. ПОРЯДОК ПЕРЕСМОТРА НАСТОЯЩЕГО ПОРЯДКА

13.1. Настоящий Порядок подлежит пересмотру:

– при изменении законодательства Российской Федерации и обязательных требований в области защиты информации;

– при изменении локальных нормативных актов Учреждения;

– при изменении состава, архитектуры и условий эксплуатации информационных систем Учреждения;

– при изменении мест размещения оборудования и машинных носителей информации;

– по результатам контроля, проверок, аудитов, расследования компьютерных инцидентов и нарушений требований физической защиты;

– при необходимости уточнения мер и условий физической защиты.

13.2. Плановый пересмотр настоящего Порядка осуществляется не реже одного раза в 3 года.

13.3. Подготовку предложений по актуализации настоящего Порядка организуют работники, ответственные за ИБ.

Приложение № 9
к Внутреннему стандарту по защите информации

Порядок вывода в контур промышленной эксплуатации сервисов, доступ к которым осуществляется с использованием телекоммуникационной сети «Интернет»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Порядок вывода в контур промышленной эксплуатации сервисов, доступ к которым осуществляется с использованием сети «Интернет» (далее – Порядок), определяет условия, этапы, требования и порядок принятия решений о выводе в контур промышленной эксплуатации сервисов, эксплуатируемых ГАПОУ СО «Балаковский политехнический техникум» (далее – Учреждение), доступ к которым осуществляется с использованием сети «Интернет».

1.2. Настоящий Порядок разработан в целях обеспечения безопасного ввода в эксплуатацию интернет-доступных сервисов, предупреждения вывода в эксплуатацию сервисов, не соответствующих требованиям по защите информации, а также обеспечения устойчивого и контролируемого функционирования таких сервисов после начала их использования.

1.3. Настоящий Порядок является локальным нормативным актом Учреждения в области защиты информации и обязателен для исполнения работниками Учреждения в пределах их компетенции.

1.4. Для целей настоящего Порядка под контуром промышленной эксплуатации понимается рабочая среда сервиса, используемая пользователями для решения задач в штатном режиме с использованием актуальных данных.

1.5. Для целей настоящего Порядка под сервисом понимается информационный ресурс, веб-приложение, сайт с интерактивными функциями, личный кабинет, образовательная платформа, программный модуль, API либо иной программный сервис, эксплуатируемый Учреждением, доступ к которому осуществляется с использованием телекоммуникационной сети «Интернет» (далее – сеть «Интернет»).

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1. Требования настоящего Порядка распространяются на сервисы, эксплуатируемые Учреждением, доступ к которым осуществляется с использованием сети «Интернет», независимо от их функционального назначения, состава пользователей и объема обрабатываемой информации.

2.2. Настоящий Порядок применяется в отношении:

– сервисов, создаваемых или внедряемых в Учреждении;

– сервисов, переводимых из тестовой, опытной или иной непроизводственной среды в контур промышленной эксплуатации;

– сервисов, в отношении которых производится существенное изменение архитектуры, состава функций, способов доступа, состава пользователей либо состава обрабатываемой информации;

– сервисов, выводимых в повторную промышленную эксплуатацию после приостановления их использования.

2.3. Требования настоящего Порядка распространяются на работников, ответственных за ИБ, работников, ответственных за эксплуатацию, иных работников Учреждения, участвующих в разработке, настройке, тестировании, сопровождении и вводе сервиса в эксплуатацию, а также на работников подрядных организаций в части выполняемых ими работ.

3. ОБЩИЕ УСЛОВИЯ ВЫВОДА СЕРВИСА В КОНТУР ПРОМЫШЛЕННОЙ ЭКСПЛУАТАЦИИ

3.1. Вывод сервиса в контур промышленной эксплуатации допускается только при наличии документально подтвержденной необходимости использования такого сервиса в деятельности Учреждения.

3.2. До вывода сервиса в контур промышленной эксплуатации должны быть определены его назначение, состав основных функций, категории пользователей, состав обрабатываемой информации, состав программных и программно-аппаратных средств, используемых при его функционировании, а также лица, участвующие в его эксплуатации и обеспечении защиты информации.

3.3. Вывод сервиса в контур промышленной эксплуатации возможен только после подтверждения его готовности к безопасному функционированию, в том числе после проведения необходимых проверок, тестирования и оценки соответствия требованиям локальных нормативных актов Учреждения.

3.4. Не допускается вывод в контур промышленной эксплуатации сервиса, если:

– не определены цели и условия его использования;

– не определен состав обрабатываемой информации;

– не определены пользователи сервиса и условия предоставления им доступа;

– не реализованы обязательные меры защиты информации;

– не устранены выявленные недостатки, препятствующие безопасной эксплуатации сервиса, либо не определены достаточные компенсирующие меры;

– отсутствует возможность сопровождения и контроля сервиса в процессе его эксплуатации.

4. ОСНОВНЫЕ ЭТАПЫ ВЫВОДА СЕРВИСА В КОНТУР ПРОМЫШЛЕННОЙ ЭКСПЛУАТАЦИИ

4.1. Вывод сервиса в контур промышленной эксплуатации осуществляется поэтапно в целях подтверждения его готовности к безопасной эксплуатации, доступности для пользователей и соответствия требованиям локальных нормативно-правовых актов Учреждения в области ИБ.

4.2. Процесс вывода сервиса в контур промышленной эксплуатации включает:

– инициирование вывода сервиса;

– подготовку сервиса к эксплуатации;

– проверку готовности сервиса;

– тестирование сервиса;

– оценку результатов тестирования и готовности сервиса;

– принятие решения о выводе сервиса в контур промышленной эксплуатации;

– ввод сервиса в контур промышленной эксплуатации;

– контроль функционирования сервиса после вывода.

5. ИНИЦИИРОВАНИЕ ВЫВОДА СЕРВИСА В КОНТУР ПРОМЫШЛЕННОЙ ЭКСПЛУАТАЦИИ

5.1. Инициирование вывода сервиса в контур промышленной эксплуатации осуществляется структурным подразделением Учреждения, заинтересованным в использовании сервиса, либо работниками, ответственными за эксплуатацию.

5.2. На этапе инициирования должны быть определены:

– наименование сервиса;

– назначение сервиса;

– предполагаемые пользователи сервиса;

– состав функций сервиса;

– наличие доступа к сервису через сеть «Интернет»;

– состав обрабатываемой информации;

– предполагаемые сроки вывода сервиса в контур промышленной эксплуатации;

– работники, ответственные за эксплуатацию.

5.3. Если сервис предполагает обработку персональных данных либо иной информации ограниченного доступа, необходимость вывода такого сервиса в контур промышленной эксплуатации рассматривается с учетом требований законодательства Российской Федерации и локальных нормативно-правовых актов Учреждения в области защиты информации, в том числе защиты информации ограниченного доступа.

6. ПОДГОТОВКА СЕРВИСА К ЭКСПЛУАТАЦИИ

6.1. Подготовка сервиса к эксплуатации осуществляется в целях обеспечения его функциональной, организационной и технической готовности к использованию в реальных условиях.

6.2. На этапе подготовки должны быть выполнены мероприятия по:

– определению архитектуры сервиса и его взаимодействия с иными ИС;

– определению состава используемых программных и программно-аппаратных средств;

– определению места размещения компонентов сервиса;

– определению порядка предоставления доступа пользователям;

– настройке параметров функционирования и безопасности;

– определению необходимых средств защиты информации;

– подготовке эксплуатационной и организационной документации, необходимой для ввода сервиса в эксплуатацию и его дальнейшего сопровождения.

6.3. Если сервис предполагает использование личных кабинетов, механизмов регистрации, аутентификации либо разграничения доступа между различными категориями пользователей, до вывода такого сервиса в контур промышленной эксплуатации должны быть определены соответствующие правила и ограничения доступа.

7. ПРОВЕРКА ГОТОВНОСТИ СЕРВИСА

7.1. До вывода сервиса в контур промышленной эксплуатации должна быть проведена проверка его готовности к использованию в штатном режиме.

7.2. Проверка готовности сервиса направлена на подтверждение того, что сервис может использоваться по назначению без создания недопустимых рисков для информации, ИС и пользователей.

7.3. В ходе проверки готовности оцениваются:

– полнота настройки сервиса;

– корректность реализации функций, необходимых для его использования;

– корректность предоставления и разграничения доступа;

– наличие и работоспособность предусмотренных мер защиты информации;

– корректность настроек безопасности;

– наличие актуальных обновлений;

– отсутствие очевидных недостатков, препятствующих безопасной эксплуатации сервиса;

– готовность работников, ответственных за эксплуатацию, к сопровождению сервиса.

8. ТЕСТИРОВАНИЕ СЕРВИСА

8.1. До вывода сервиса в контур промышленной эксплуатации сервис подлежит тестированию.

8.2. Тестирование проводится в целях подтверждения корректности функционирования сервиса, устойчивости его работы, правильности предоставления доступа пользователям, а также отсутствия недостатков, препятствующих безопасной эксплуатации.

8.3. В рамках тестирования проверяются:

– корректность работы основных функций сервиса;

– корректность регистрации, аутентификации и предоставления доступа пользователям, если такие функции предусмотрены;

– корректность разграничения доступа между различными категориями пользователей;

– корректность обработки, хранения и передачи информации;

– корректность работы средств защиты информации;

– корректность журналирования событий, если оно предусмотрено;

– устойчивость сервиса после настройки, обновления или изменения его конфигурации;

– устранение выявленных ранее недостатков и уязвимостей.

8.4. При необходимости в рамках тестирования могут проводиться дополнительные проверки, связанные с особенностями конкретного сервиса, его архитектуры, объема обрабатываемой информации и условий эксплуатации.

9. ТРЕБОВАНИЯ К ЗАЩИТЕ ИНФОРМАЦИИ ПРИ ВЫВОДЕ СЕРВИСА

9.1. До вывода сервиса в контур промышленной эксплуатации должны быть определены и реализованы меры защиты информации, соответствующие назначению сервиса, условиям его эксплуатации, составу пользователей и объему обрабатываемой информации.

9.2. При оценке готовности сервиса должно быть установлено:

– какие сведения обрабатываются в сервисе;

– кто является пользователями сервиса;

– каким образом предоставляется, изменяется и прекращается доступ к сервису;

– каким образом обеспечивается идентификация и аутентификация пользователей;

– каким образом реализуется разграничение доступа;

– каким образом обеспечивается защита данных при передаче через сеть «Интернет»;

– каким образом осуществляется сопровождение, обновление и контроль сервиса;

– каким образом осуществляется реагирование на нарушения и инциденты информационной безопасности.

9.3. Если сервис доступен через сеть «Интернет», должны быть приняты меры, исключающие либо существенно затрудняющие:

– несанкционированный доступ к сервису;

– доступ пользователей к функциям и данным сверх предоставленных им полномочий;

– использование уязвимостей сервиса;

– компрометацию учетных данных пользователей;

– нарушение конфиденциальности, целостности и доступности информации.

9.4. Не допускается вывод в контур промышленной эксплуатации сервиса при наличии неустраненных критических недостатков безопасности либо при отсутствии мер, позволяющих исключить недопустимые риски для информации и ИС.

10. ОЦЕНКА ГОТОВНОСТИ СЕРВИСА И ПРИНЯТИЕ РЕШЕНИЯ

10.1. Оценка готовности сервиса к выводу в контур промышленной эксплуатации осуществляется работниками, ответственными за ИБ, во взаимодействии с работниками, ответственными за эксплуатацию.

10.2. При необходимости по решению Учреждения для оценки готовности сервиса может создаваться комиссия.

10.3. По результатам оценки готовности сервиса принимается одно из следующих решений:

– сервис готов к выводу в контур промышленной эксплуатации;

– сервис готов к выводу в контур промышленной эксплуатации при условии устранения отдельных замечаний;

– сервис не готов к выводу в контур промышленной эксплуатации.

10.4. При принятии решения учитываются результаты проверки готовности, тестирования, оценки реализованных мер защиты информации, сведения о выявленных уязвимостях, готовность работников, ответственных за эксплуатацию, а также наличие либо отсутствие замечаний, препятствующих безопасной эксплуатации сервиса.

10.5. Решение о выводе сервиса в контур промышленной эксплуатации оформляется в порядке, установленном в Учреждении.

11. ВВОД СЕРВИСА В КОНТУР ПРОМЫШЛЕННОЙ ЭКСПЛУАТАЦИИ

11.1. После принятия положительного решения сервис переводится в контур промышленной эксплуатации и допускается к использованию реальными пользователями в штатном режиме.

11.2. До начала фактического использования сервиса должны быть определены:

– порядок сопровождения сервиса;

– порядок предоставления и прекращения доступа пользователям;

– порядок внесения изменений в сервис;

– порядок реагирования на нарушения и инциденты информационной безопасности;

– порядок временного ограничения либо приостановления эксплуатации сервиса при выявлении существенных недостатков.

11.3. После вывода сервиса в контур промышленной эксплуатации его эксплуатация осуществляется в соответствии с локальными нормативными актами Учреждения, регулирующими доступ к ИС, защиту информации, управление уязвимостями, применение обновлений и иные связанные процессы.

12. КОНТРОЛЬ ФУНКЦИОНИРОВАНИЯ СЕРВИСА ПОСЛЕ ВЫВОДА

12.1. После вывода сервиса в контур промышленной эксплуатации осуществляется контроль его функционирования в целях своевременного выявления недостатков, нарушений и иных обстоятельств, способных повлиять на безопасность информации или устойчивость работы сервиса.

12.2. Контроль функционирования сервиса включает:

– анализ стабильности работы сервиса;

– анализ ошибок и недостатков, выявленных в ходе эксплуатации;

– контроль соблюдения установленной конфигурации;

– контроль уязвимостей и обновлений;

– контроль соблюдения порядка предоставления доступа пользователям;

– анализ нарушений безопасности информации и событий, способных привести к компьютерным инцидентам.

12.3. При выявлении после вывода сервиса в контур промышленной эксплуатации существенных недостатков, критических уязвимостей либо нарушений требований безопасности информации может быть принято решение:

– о введении временных ограничений эксплуатации;

– о приостановлении отдельных функций сервиса;

– о временном выводе сервиса из контура промышленной эксплуатации;

– о необходимости выполнения дополнительных организационных и технических мер.

13. ОТВЕТСТВЕННОСТЬ

13.1. Работники, ответственные за эксплуатацию, несут ответственность за выполнение мероприятий по подготовке сервиса к эксплуатации, сопровождению сервиса и соблюдению требований настоящего Порядка в пределах своей компетенции.

13.2. Работники, ответственные за ИБ, несут ответственность за участие в оценке готовности сервиса, проверке соблюдения требований по защите информации, подготовке предложений по устранению выявленных недостатков и контролю соблюдения настоящего Порядка в пределах своей компетенции.

13.3. Руководители структурных подразделений Учреждения несут ответственность за обоснованность инициирования вывода сервиса в контур промышленной эксплуатации и организацию выполнения мероприятий, отнесенных к их компетенции.

14. ПОРЯДОК ПЕРЕСМОТРА

14.1. Настоящий Порядок подлежит пересмотру при изменении законодательства Российской Федерации, обязательных требований в области защиты информации, локальных нормативных актов Учреждения, архитектуры и состава интернет-доступных сервисов, а также по результатам проверок, аудитов, оценки защищенности и расследования компьютерных инцидентов.

14.2. Плановый пересмотр настоящего Порядка осуществляется не реже одного раза в 3 года.

14.3. Подготовку предложений по актуализации настоящего Порядка организуют работники, ответственные за ИБ.

Приложение № 10
к Внутреннему стандарту по защите информации

Порядок восстановления штатного функционирования информационных систем и тестирования процессов восстановления

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Порядок восстановления штатного функционирования информационных систем и тестирования процессов восстановления (далее – Порядок) определяет условия, последовательность действий и основные требования к восстановлению штатного функционирования ИС, эксплуатируемых ГАПОУ СО «Балаковский политехнический техникум» (далее – Учреждение), а также к организации и проведению тестирования процессов восстановления.

1.2. Настоящий Порядок разработан в целях обеспечения возможности своевременного восстановления штатного функционирования ИС после сбоев, отказов, нарушений работоспособности, компьютерных инцидентов, ошибок эксплуатации, нарушений целостности данных, повреждения программных и программно-аппаратных средств и иных событий, способных повлиять на функционирование ИС.

1.3. Настоящий Порядок является локальным нормативным актом Учреждения в области защиты информации и обязателен для исполнения работниками Учреждения в пределах их компетенции.

1.4. Для целей настоящего Порядка под восстановлением штатного функционирования понимается выполнение организационных и технических мероприятий, направленных на возврат ИС в состояние, при котором обеспечивается их работоспособность, доступность, корректность обработки информации и возможность дальнейшей безопасной эксплуатации.

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1. Требования настоящего Порядка распространяются на:

– федеральные, государственные, региональные, объектовые и иные ИС, эксплуатируемые Учреждением;

– программные и программно-аппаратные средства, входящие в состав ИС;

– автоматизированные рабочие места, серверы, сетевое оборудование, средства хранения данных, средства виртуализации и иные компоненты ИС;

– программное обеспечение, базы данных, конфигурации, учетные записи, журналы событий и иные элементы, необходимые для штатного функционирования ИС;

– работников, ответственных за ИБ;

– работников, ответственных за эксплуатацию;

– иных работников Учреждения, участвующих в сопровождении, восстановлении и контроле функционирования ИС.

2.2. Настоящий Порядок применяется:

– при возникновении сбоев и отказов;

– при нарушении доступности ИС либо отдельных ее компонентов;

– при повреждении, утрате или искажении данных;

– после компьютерных инцидентов;

– после ошибочных действий пользователей;

– после сбоев электропитания, отказов оборудования, сбоев программного обеспечения и иных событий, способных повлиять на функционирование ИС;

– при проведении планового тестирования процессов восстановления.

3. ЦЕЛИ И ОБЩИЕ ПРИНЦИПЫ ВОССТАНОВЛЕНИЯ

3.1. Восстановление штатного функционирования ИС осуществляется в целях:

– минимизации времени простоя ИС;

– восстановления работоспособности ИС и ее компонентов;

– восстановления доступа к информации, необходимой для функционирования ИС;

– обеспечения корректности дальнейшей обработки информации;

– исключения повторного ввода ИС в эксплуатацию при наличии неустраненных критических нарушений.

3.2. Восстановление штатного функционирования ИС осуществляется на основании следующих принципов:

– своевременности;

– поэтапности;

– приоритетности восстановления наиболее значимых функций;

– контролируемости выполняемых действий;

– документируемости решений и результатов;

– обязательной проверки корректности восстановления до возвращения ИС в штатный режим эксплуатации.

4. ОРГАНИЗАЦИЯ ВОССТАНОВЛЕНИЯ ШТАТНОГО ФУНКЦИОНИРОВАНИЯ

4.1. Организацию мероприятий по восстановлению штатного функционирования ИС осуществляют работники, ответственные за ИБ, во взаимодействии с работниками, ответственными за эксплуатацию.

4.2. Работники, ответственные за ИБ:

– участвуют в оценке характера события, повлиявшего на функционирование ИС;

– определяют необходимость введения временных ограничений;

– участвуют в определении безопасного порядка восстановления;

– контролируют соблюдение требований по защите информации в ходе восстановления;

– участвуют в оценке готовности ИС к возврату в штатный режим эксплуатации.

4.3. Работники, ответственные за эксплуатацию:

– выявляют признаки нарушения функционирования ИС;

– осуществляют первичные действия по локализации последствий;

– выполняют мероприятия по восстановлению программных, программно-аппаратных и иных компонентов ИС;

– проводят проверку работоспособности после восстановления;

– информируют работников, ответственных за ИБ, о ходе и результатах восстановления.

4.4. При необходимости по решению Учреждения для координации мероприятий по восстановлению может создаваться комиссия либо определяться состав работников, участвующих в восстановлении конкретной ИС.

5. ОСНОВАНИЯ ДЛЯ НАЧАЛА ВОССТАНОВЛЕНИЯ

5.1. Основанием для начала мероприятий по восстановлению штатного функционирования ИС является выявление события, повлекшего либо способного повлечь:

– прекращение функционирования ИС;

– нарушение работоспособности ИС либо ее отдельных компонентов;

– нарушение доступности информации;

– нарушение целостности данных;

– невозможность использования ИС пользователями информационных систем;

– невозможность выполнения ИС своих функций в установленном режиме.

5.2. При выявлении признаков нарушения функционирования ИС работники, ответственные за эксплуатацию, обязаны незамедлительно:

– оценить характер нарушения;

– принять меры по исключению дальнейшего ухудшения состояния ИС;

– проинформировать работников, ответственных за ИБ;

– при необходимости ограничить использование ИС либо ее отдельных функций до завершения восстановления.

5.3. Если нарушение функционирования ИС связано с компьютерным инцидентом, восстановление осуществляется с учетом необходимости сохранения сведений о таком инциденте, результатов анализа и иных материалов, необходимых для его расследования.

6. ОСНОВНЫЕ ЭТАПЫ ВОССТАНОВЛЕНИЯ ШТАТНОГО ФУНКЦИОНИРОВАНИЯ

6.1. Восстановление штатного функционирования ИС осуществляется поэтапно и должно обеспечивать возврат ИС в состояние, пригодное для безопасной и корректной эксплуатации.

6.2. Процесс восстановления включает:

– выявление и первичную оценку нарушения;

– локализацию последствий нарушения;

– определение состава затронутых компонентов ИС;

– определение способа восстановления;

– выполнение восстановительных мероприятий;

– проверку работоспособности и корректности функционирования ИС;

– принятие решения о возврате ИС в штатный режим эксплуатации;

– контроль функционирования ИС после восстановления.

6.3. Выявление и первичная оценка нарушения

6.3.1 На этапе выявления и первичной оценки устанавливаются:

– характер нарушения;

– затронутые компоненты ИС;

– возможные причины нарушения;

– влияние нарушения на доступность, целостность и корректность функционирования ИС;

– необходимость введения временных ограничений на использование ИС.

6.4. Локализация последствий нарушения

6.4.1 На этапе локализации последствий принимаются меры, направленные на предотвращение дальнейшего распространения последствий нарушения, в том числе:

– ограничение доступа к затронутым компонентам;

– временное отключение отдельных функций;

– изоляция неисправных либо скомпрометированных компонентов;

– сохранение резервных копий и иных данных, необходимых для восстановления;

– предотвращение повторного возникновения нарушения на этапе восстановления.

6.5. Определение способа восстановления

6.5.1. Способ восстановления определяется исходя из характера нарушения и может включать:

– перезапуск сервиса, компонента либо ИС в целом;

– восстановление конфигурации;

– замену либо переключение на резервный компонент;

– восстановление данных из резервной копии;

– установку исправлений, обновлений или корректирующих настроек;

– повторное развертывание программного обеспечения;

– иные мероприятия, необходимые для возврата ИС в работоспособное состояние.

6.6. Выполнение восстановительных мероприятий

6.6.1 В ходе выполнения восстановительных мероприятий должны обеспечиваться:

– контролируемость выполняемых действий;

– исключение несанкционированного доступа к ИС и информации;

– сохранение целостности восстанавливаемых данных;

– соблюдение требований локальных нормативных актов Учреждения.

6.7. Проверка результатов восстановления

6.7.1 После завершения восстановительных мероприятий обязательно проводится проверка результатов восстановления.

6.8. В ходе проверки должно быть установлено:

– восстановлена ли работоспособность ИС;

– функционируют ли основные компоненты ИС корректно;

– восстановлена ли доступность информации в необходимом объеме;

– отсутствуют ли признаки повторного нарушения;

– могут ли пользователи информационных систем безопасно использовать ИС по назначению.

7. ВОЗВРАТ ИС В ШТАТНЫЙ РЕЖИМ ЭКСПЛУАТАЦИИ

7.1. ИС может быть возвращена в штатный режим эксплуатации только после подтверждения того, что:

– восстановлены необходимые функции ИС;

– устранены либо локализованы причины нарушения функционирования;

– исключены либо снижены до допустимого уровня риски повторного нарушения;

– обеспечена возможность дальнейшей безопасной эксплуатации ИС.

7.2. Решение о возврате ИС в штатный режим эксплуатации принимается в порядке, установленном в Учреждении, с участием работников, ответственных за ИБ, и работников, ответственных за эксплуатацию.

7.3. Если по результатам восстановления установлено, что ИС может функционировать только с ограничениями, допускается ее временная эксплуатация в ограниченном режиме до полного устранения выявленных недостатков.

8. ТЕСТИРОВАНИЕ ПРОЦЕССОВ ВОССТАНОВЛЕНИЯ

8.1. Тестирование процессов восстановления проводится в целях проверки готовности Учреждения к восстановлению штатного функционирования ИС, оценки достаточности принятых организационных и технических мер, а также выявления недостатков в порядке восстановления.

8.2. Тестирование процессов восстановления должно быть направлено на подтверждение того, что при возникновении нарушения функционирования ИС Учреждение способно:

– своевременно выявить нарушение;

– определить затронутые компоненты;

– организовать взаимодействие между работниками, ответственными за ИБ, и работниками, ответственными за эксплуатацию;

– выполнить мероприятия по восстановлению;

– проверить результаты восстановления;

– вернуть ИС в штатный либо допустимо ограниченный режим эксплуатации.

8.3. Тестирование процессов восстановления может проводиться:

– в плановом порядке;

– при вводе в эксплуатацию новых ИС либо существенном изменении их архитектуры;

– после компьютерных инцидентов;

– после существенных изменений порядка резервного копирования, конфигурации либо состава ИС;

– при необходимости проверки готовности к восстановлению конкретной ИС.

8.4. В рамках тестирования процессов восстановления могут проверяться:

– восстановление работоспособности отдельных компонентов ИС;

– восстановление конфигураций;

– восстановление данных из резервных копий;

– восстановление доступа пользователей;

– переключение на резервные компоненты;

– корректность взаимодействия между работниками, участвующими в восстановлении;

– соблюдение последовательности действий, предусмотренной настоящим Порядком.

8.5. По результатам тестирования процессов восстановления оцениваются:

– полнота и корректность порядка восстановления;

– достаточность имеющихся ресурсов для восстановления;

– достаточность резервных копий, конфигурационных данных и иных средств восстановления;

– наличие недостатков, препятствующих своевременному восстановлению;

– необходимость корректировки локальных нормативно-правовых актов Учреждения, настроек ИС либо организационных мероприятий.

9. РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ И КОРРЕКТИРУЮЩИЕ МЕРЫ

9.1. Результаты тестирования процессов восстановления подлежат анализу работниками, ответственными за ИБ, и работниками, ответственными за эксплуатацию.

9.2. Если по результатам тестирования выявлены недостатки, должны быть определены корректирующие меры, направленные на:

– уточнение последовательности действий по восстановлению;

– изменение состава резервируемых данных;

– изменение состава и параметров резервных компонентов;

– изменение конфигурации ИС;

– уточнение обязанностей работников, участвующих в восстановлении;

– повышение готовности к восстановлению в иных формах, необходимых для конкретной ИС.

9.3. При необходимости результаты тестирования процессов восстановления учитываются при пересмотре настоящего Порядка и иных локальных нормативных актов Учреждения.

10. ДОКУМЕНТИРОВАНИЕ МЕРОПРИЯТИЙ ПО ВОССТАНОВЛЕНИЮ

10.1. Отдельный журнал настоящим Порядком не вводится.

10.2. Сведения о случаях восстановления штатного функционирования ИС и о результатах тестирования процессов восстановления фиксируются в документах, применяемых в Учреждении, в том числе:

– в служебных записках;

– в актах;

– в документах по расследованию компьютерных инцидентов;

– в эксплуатационной документации;

– в иных документах, применяемых в Учреждении.

10.3. В документах по результатам восстановления либо тестирования процессов восстановления, при необходимости, отражаются:

– дата и основание проведения мероприятий;

– затронутая ИС и ее компоненты;

– характер нарушения либо сценарий тестирования;

– выполненные действия;

– результаты проверки работоспособности;

– вывод о возможности штатной эксплуатации;

– выявленные недостатки и корректирующие меры.

11. ОТВЕТСТВЕННОСТЬ

11.1. Работники, ответственные за эксплуатацию, несут ответственность за своевременное выявление нарушений функционирования ИС, выполнение восстановительных мероприятий и информирование о ходе восстановления в пределах своей компетенции.

11.2. Работники, ответственные за ИБ, несут ответственность за участие в оценке характера нарушения, контроле соблюдения требований по защите информации при восстановлении, анализе результатов тестирования процессов восстановления и подготовке предложений по совершенствованию настоящего Порядка в пределах своей компетенции.

11.3. Руководители структурных подразделений Учреждения несут ответственность за организацию выполнения мероприятий по восстановлению штатного функционирования ИС в пределах своей компетенции.

12. ПОРЯДОК ПЕРЕСМОТРА

12.1. Настоящий Порядок подлежит пересмотру при изменении законодательства Российской Федерации, обязательных требований в области защиты информации, локальных нормативных актов Учреждения, состава и архитектуры ИС, а также по результатам проверок, аудитов, компьютерных инцидентов и тестирования процессов восстановления.

12.2. Плановый пересмотр настоящего Порядка осуществляется не реже одного раза в 3 года.

12.3. Подготовку предложений по актуализации настоящего Порядка организуют работники, ответственные за ИБ.

Приложение № 11
к Внутреннему стандарту по защите информации

Порядок мониторинга информационной безопасности информационных систем

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Порядок мониторинга информационной безопасности информационных систем (далее – Порядок) определяет цели, задачи, содержание, условия и порядок организации мониторинга информационной безопасности ИС, эксплуатируемых ГАПОУ СО «Балаковский политехнический техникум» (далее – Учреждение).

1.2. Настоящий Порядок разработан в целях обеспечения своевременного выявления событий безопасности, признаков реализации угроз безопасности информации, нарушений требований локальных нормативных актов Учреждения в области защиты информации, а также в целях повышения устойчивости и защищенности ИС.

1.3. Настоящий Порядок является локальным нормативным актом Учреждения в области защиты информации и обязателен для исполнения работниками Учреждения в пределах их компетенции.

1.4. Для целей настоящего Порядка под мониторингом информационной безопасности понимается совокупность организационных и технических мероприятий, направленных на сбор данных о событиях безопасности, их обработку, анализ и выявление признаков реализации угроз безопасности информации, нарушений требований по защите информации и иных обстоятельств, способных повлиять на безопасность информации и функционирование ИС.

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1. Требования настоящего Порядка распространяются на федеральные, государственные, объектовые и иные ИС, эксплуатируемые Учреждением, а также на программные, программно-аппаратные средства и компоненты, входящие в их состав.

2.2. Настоящий Порядок распространяется на:

– серверы, автоматизированные рабочие места, сетевое оборудование, средства хранения данных, средства виртуализации и иные компоненты ИС;

– средства защиты информации, применяемые в ИС;

– учетные записи пользователей информационных систем;

– журналы регистрации событий, средства сбора и анализа событий безопасности;

– работников, ответственных за ИБ;

– работников, ответственных за эксплуатацию;

– иных работников Учреждения в части, касающейся выполнения ими требований настоящего Порядка.

2.3. Мероприятия по мониторингу информационной безопасности должны проводиться в отношении всех ИС, за исключением локальных и изолированных ИС. В локальных и изолированных ИС должен обеспечиваться контроль журналов регистрации событий безопасности.

3. ЦЕЛИ И ЗАДАЧИ МОНИТОРИНГА ИБ

3.1. Мониторинг информационной безопасности осуществляется в целях:

– своевременного выявления событий безопасности;

– выявления признаков реализации угроз безопасности информации;

– выявления нарушений требований локальных нормативных актов Учреждения в области защиты информации;

– своевременного обнаружения предпосылок возникновения компьютерных инцидентов;

– получения сведений, необходимых для реагирования на нарушения безопасности информации;

– подготовки предложений по совершенствованию мер защиты информации.

3.2. Основными задачами мониторинга информационной безопасности являются:

– сбор данных о событиях безопасности;

– обработка и анализ полученных данных;

– выявление отклонений от штатного режима функционирования ИС;

– выявление аномальной, подозрительной и потенциально опасной активности;

– выявление признаков нарушений порядка предоставления доступа, удаленного доступа, использования сети «Интернет», применения привилегированных учетных записей и иных процессов, регулируемых локальными нормативными актами Учреждения;

– формирование сведений для анализа, реагирования и отчетности.

4. ОРГАНИЗАЦИЯ МОНИТОРИНГА ИБ

4.1. Организация мониторинга информационной безопасности осуществляется работниками, ответственных за ИБ, во взаимодействии с работниками, ответственными за эксплуатацию.

4.2. Работники, ответственные за ИБ:

– организуют мероприятия по мониторингу информационной безопасности;

– определяют состав анализируемых событий безопасности;

– осуществляют обработку и анализ данных мониторинга;

– выявляют признаки реализации угроз безопасности информации и нарушений требований локальных нормативных актов Учреждения;

– подготавливают предложения по реагированию на выявленные события и отклонения;

– подготавливают отчетность по результатам мониторинга.

4.3. Работники, ответственные за эксплуатацию:

– обеспечивают техническую возможность регистрации и передачи событий безопасности;

– обеспечивают функционирование средств журналирования, сбора и передачи событий;

– участвуют в анализе выявленных нарушений и отклонений;

– исполняют мероприятия, направленные на устранение причин выявленных нарушений, в пределах своей компетенции;

– информируют работников, ответственных за ИБ, о событиях, способных повлиять на безопасность информации и функционирование ИС.

4.4. В Учреждении для выполнения обязанностей по мониторингу информационной безопасности могут применяться программные и программно-аппаратные средства, предназначенные для автоматизации и аналитической поддержки деятельности по защите информации.

5. ОБЪЕКТЫ И ИСТОЧНИКИ МОНИТОРИНГА ИБ

5.1. 5.1. Мониторингу подлежат события безопасности, связанные с функционированием ИС, действиями пользователей информационных систем, функционированием средств защиты информации и иными процессами, способными повлиять на безопасность информации.

5.2. 5.2. В рамках мониторинга могут учитываться сведения:

– о попытках входа пользователей;

– о действиях пользователей с учетными записями;

– о действиях с привилегированными учетными записями;

– о предоставлении, изменении, блокировании и прекращении доступа;

– о событиях, связанных с удаленным доступом;

– о событиях, связанных с доступом из ИС в сеть «Интернет»;

– о срабатывании средств защиты информации;

– о нарушении штатного функционирования компонентов ИС;

– о выявленных уязвимостях, сбоях и отказах;

– о попытках изменения конфигурации;

– о событиях, способных свидетельствовать о компьютерном инциденте.

5.3. Источниками сведений для мониторинга являются:

– журналы регистрации событий безопасности;

– журналы операционных систем, прикладного программного обеспечения и средств защиты информации;

– сведения о функционировании сетевого оборудования и серверов;

– результаты контроля конфигураций;

– результаты контроля уязвимостей;

– результаты анализа привилегированного доступа;

– результаты контроля удаленного доступа и доступа в сеть «Интернет»;

– иные данные, используемые в Учреждении для обеспечения защиты информации.

6. СБОР, ОБРАБОТКА И АНАЛИЗ СОБЫТИЙ ИБ

6.1. Мониторинг информационной безопасности должен обеспечивать непрерывный либо периодический сбор данных о событиях безопасности в объеме, достаточном для анализа состояния защищенности ИС и выявления признаков нарушений.

6.2. Сбор данных о событиях безопасности осуществляется с использованием предусмотренных в Учреждении средств журналирования, регистрации, передачи, накопления и анализа событий безопасности.

6.3. Полученные данные подлежат обработке и анализу в целях:

– выявления событий, требующих дополнительного рассмотрения;

– выявления взаимосвязанных событий;

– выявления отклонений от обычного поведения пользователей и компонентов ИС;

– выявления признаков реализации угроз безопасности информации;

– выявления нарушений требований локальных нормативных актов Учреждения.

6.4. Анализ событий безопасности может осуществляться как вручную, так и с применением автоматизированных средств.

7. ВЫЯВЛЕНИЕ ПРИЗНАКОВ УГРОЗ И НАРУШЕНИЙ

7.1. В ходе мониторинга информационной безопасности должны выявляться признаки:

– несанкционированного доступа;

– неправомерного использования учетных записей;

– нарушений порядка использования привилегированных учетных записей;

– нарушений порядка удаленного доступа;

– нарушений порядка предоставления пользователям доступа из ИС в сеть «Интернет»;

– нарушения конфигурации, способного повлиять на безопасность информации;

– аномальной либо подозрительной активности пользователей информационных систем;

– признаков эксплуатации уязвимостей;

– нарушений штатного функционирования ИС;

– иных событий, указывающих на возможную реализацию угроз безопасности информации.

7.2. При выявлении признаков нарушений либо угроз работники, ответственные за ИБ, организуют их дополнительный анализ и при необходимости инициируют принятие мер реагирования, предусмотренных локальными нормативными актами Учреждения.

8. ОСОБЕННОСТИ МОНИТОРИНГА ЛОКАЛЬНЫХ И ИЗОЛИРОВАННЫХ ИС

8.1. В отношении локальных и изолированных ИС мероприятия по мониторингу информационной безопасности в полном объеме могут не проводиться.

8.2. В локальных и изолированных ИС должен обеспечиваться контроль журналов регистрации событий безопасности в объеме, достаточном для выявления нарушений безопасности информации и нарушений функционирования ИС.

8.3. Порядок и периодичность такого контроля определяются Учреждением с учетом особенностей соответствующей ИС, состава обрабатываемой информации и характера возможных угроз.

9. ОТЧЕТНОСТЬ ПО РЕЗУЛЬТАТАМ МОНИТОРИНГА

9.1. Работники, ответственные за ИБ, с периодичностью и в сроки, установленные настоящим Порядком, подготавливают и представляют директору Учреждения либо уполномоченному лицу отчет о результатах мониторинга информационной безопасности.

9.2. Отчет о результатах мониторинга должен содержать, в том числе:

– типы событий безопасности, обнаруженные по результатам мониторинга;

– сведения о связанных с ними компьютерных инцидентах при их наличии;

– результаты анализа выявленных событий;

– рекомендации по анализу, устранению причин и снижению рисков повторения таких событий.

9.3. Текущие отчеты о результатах мониторинга подготавливаются ежеквартально.

9.4. Итоговый отчет о результатах мониторинга за текущий год подготавливается по итогам календарного года.

9.5. Последний в текущем году отчет о результатах мониторинга либо итоговый отчет за текущий год после представления директору Учреждения направляется в ФСТЭК России.

10. РЕАГИРОВАНИЕ ПО РЕЗУЛЬТАТАМ МОНИТОРИНГА

10.1. По результатам мониторинга информационной безопасности в Учреждении могут приниматься решения:

– о проведении дополнительного анализа отдельных событий безопасности;

– о проверке корректности конфигурации ИС;

– о проверке прав доступа пользователей;

– о проведении мероприятий по устранению выявленных нарушений;

– о временном ограничении отдельных функций ИС;

– о проведении мероприятий по управлению уязвимостями;

– о проведении мероприятий по применению обновлений;

– о проведении служебной проверки;

– о корректировке локальных нормативных актов Учреждения.

10.2. Если по результатам мониторинга выявлены признаки компьютерного инцидента, дальнейшие действия осуществляются в соответствии с локальными нормативными актами Учреждения, регулирующими порядок реагирования на инциденты информационной безопасности и восстановления штатного функционирования ИС.

11. ДОКУМЕНТИРОВАНИЕ РЕЗУЛЬТАТОВ МОНИТОРИНГА

11.1. Отдельный журнал настоящим Порядком не вводится.

11.2. Сведения о мероприятиях по мониторингу информационной безопасности, выявленных событиях, подготовленных выводах и рекомендациях фиксируются в документах, применяемых в Учреждении, в том числе:

– в отчетах о результатах мониторинга;

– в служебных записках;

– в актах;

– в документах по расследованию компьютерных инцидентов;

– в эксплуатационной документации;

– в иных документах, применяемых в Учреждении.

11.3. При необходимости в документах по результатам мониторинга отражаются:

– анализируемая ИС либо группа ИС;

– период мониторинга;

– типы выявленных событий безопасности;

– выявленные признаки угроз и нарушений;

– сведения о связанных инцидентах;

– выводы и рекомендации по устранению выявленных нарушений и снижению рисков.

12. ОТВЕТСТВЕННОСТЬ

12.1. Работники, ответственные за ИБ, несут ответственность за организацию мониторинга информационной безопасности, анализ событий безопасности, подготовку

отчетности и формирование предложений по совершенствованию защиты информации в пределах своей компетенции.

12.2. Работники, ответственные за эксплуатацию, несут ответственность за обеспечение регистрации событий безопасности, техническую поддержку используемых средств мониторинга и исполнение мероприятий, направленных на устранение выявленных нарушений, в пределах своей компетенции.

12.3. Пользователи информационных систем обязаны соблюдать требования локальных нормативных актов Учреждения, а при выявлении признаков нарушений безопасности информации или нестандартного поведения ИС незамедлительно информировать работников, ответственных за ИБ, либо работников, ответственных за эксплуатацию.

13. ПОРЯДОК ПЕРЕСМОТРА

13.1. Настоящий Порядок подлежит пересмотру при изменении законодательства Российской Федерации, обязательных требований в области защиты информации, локальных нормативных актов Учреждения, состава и архитектуры ИС, а также по результатам проверок, аудитов, расследования компьютерных инцидентов и анализа эффективности мониторинга.

13.2. Плановый пересмотр настоящего Порядка осуществляется не реже одного раза в 3 года.

13.3. Подготовку предложений по актуализации настоящего Порядка организуют работники, ответственные за ИБ.

Приложение № 12
к Внутреннему стандарту по защите информации

Порядок контроля уровня защищенности информации, содержащейся в информационных системах

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Порядок контроля уровня защищенности информации, содержащейся в информационных системах (далее – Порядок), определяет цели, условия, методы, периодичность и порядок организации контроля уровня защищенности информации, содержащейся в ИС, эксплуатируемых ГАПОУ СО «Балаковский политехнический техникум» (далее – Учреждение).

1.2. Настоящий Порядок разработан в целях подтверждения фактического состояния защищенности информации, своевременного выявления недостатков системы защиты информации, оценки достаточности реализованных организационных и технических мер защиты информации, а также подготовки предложений по повышению уровня защищенности информации в ИС.

1.3. Настоящий Порядок является локальным нормативным актом Учреждения в области защиты информации и обязателен для исполнения работниками Учреждения в пределах их компетенции.

1.4. Требования настоящего Порядка распространяются на все ИС, эксплуатируемые Учреждением, включая информационные системы персональных данных.

1.5. Для целей настоящего Порядка под контролем уровня защищенности информации понимается проведение мероприятий по анализу защищенности ИС и тестированию системы защиты информации в целях оценки фактического состояния защиты информации и выявления необходимости доработки либо усиления принятых мер защиты информации.

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1. Требования настоящего Порядка распространяются на:

– федеральные, государственные, объектовые и иные ИС, эксплуатируемые Учреждением;

– информационные системы персональных данных, эксплуатируемые Учреждением;

– программные и программно-аппаратные средства, входящие в состав ИС;

– системы защиты информации, применяемые в ИС;

– автоматизированные рабочие места, серверы, сетевое оборудование, средства хранения данных, средства виртуализации и иные компоненты ИС;

– работников, ответственных за ИБ;

– работников, ответственных за эксплуатацию;

– иных работников Учреждения в части, касающейся выполнения ими требований настоящего Порядка.

2.2. Контроль уровня защищенности информации осуществляется в отношении ИС в целом либо их отдельных сегментов, компонентов, функций и процессов, если это необходимо с учетом архитектуры ИС, состава обрабатываемой информации и характера актуальных угроз безопасности информации.

3. ЦЕЛИ И ЗАДАЧИ КОНТРОЛЯ УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ

3.1. Контроль уровня защищенности информации осуществляется в целях:

– оценки фактического состояния защищенности информации, содержащейся в ИС;

– проверки достаточности и результативности реализованных мер защиты информации;

– выявления недостатков в функционировании системы защиты информации;

– выявления нарушений требований локальных нормативных актов Учреждения в области защиты информации;

– подготовки решений о необходимости доработки, модернизации либо усиления системы защиты информации.

3.2. Основными задачами контроля уровня защищенности информации являются:

– анализ защищенности ИС;

– тестирование системы защиты информации;

– оценка правильности реализации организационных и технических мер защиты информации;

– выявление уязвимостей, недостатков конфигурации и иных факторов, влияющих на защищенность информации;

– оценка способности системы защиты информации противодействовать актуальным угрозам;

– формирование выводов о достаточности либо недостаточности принятых мер защиты информации.

4. ОРГАНИЗАЦИЯ КОНТРОЛЯ УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ

4.1. Организацию контроля уровня защищенности информации осуществляют работники, ответственные за ИБ, во взаимодействии с работниками, ответственными за эксплуатацию.

4.2. Работники, ответственные за ИБ:

– организуют планирование и проведение контроля уровня защищенности информации;

– определяют методы контроля с учетом особенностей соответствующей ИС;

– участвуют в анализе результатов контроля;

– подготавливают выводы и предложения по повышению уровня защищенности информации;

–обеспечивают подготовку отчета по результатам контроля.

4.3. Работники, ответственные за эксплуатацию:

– обеспечивают доступ к сведениям, необходимым для проведения контроля;

– участвуют в обследовании ИС и ее компонентов;

– обеспечивают выполнение необходимых технических мероприятий в процессе контроля;

– участвуют в анализе выявленных недостатков и подготовке предложений по их устранению.

4.4. При необходимости по решению Учреждения для проведения контроля уровня защищенности информации может создаваться комиссия.

4.5. Контроль уровня защищенности информации может проводиться Учреждением самостоятельно и/или с привлечением организации, обладающей правом на выполнение соответствующих работ в области технической защиты конфиденциальной информации, если это необходимо по характеру и объему проводимых мероприятий.

5. ОСНОВАНИЯ, ПЕРИОДИЧНОСТЬ И ПЛАНИРОВАНИЕ КОНТРОЛЯ

5.1. Контроль уровня защищенности информации проводится в плановом и внеплановом порядке.

5.2. Плановый контроль проводится в соответствии с документами Учреждения, определяющими организацию работ по защите информации.

5.3. Внеплановый контроль проводится:

– после компьютерного инцидента, произошедшего в Учреждении;

– после существенного изменения архитектуры ИС;

– после существенного изменения состава программных и программно-аппаратных средств;

– после изменения системы защиты информации;

– после выявления значимых недостатков в ходе мониторинга информационной безопасности, управления уязвимостями либо восстановления штатного функционирования ИС;

– по решению руководителя Учреждения либо по предложению работников, ответственных за ИБ.

5.4. Контроль уровня защищенности информации проводится не реже одного раза в три года или после компьютерного инцидента, произошедшего в Учреждении. Методы контроля и периодичность его проведения определяются Учреждением настоящим Порядком.

5.5. При планировании контроля должны учитываться:

– значимость ИС;
– состав обрабатываемой информации;
– наличие доступа к ИС с использованием сети «Интернет»;
– изменения в конфигурации и архитектуре ИС;
– результаты ранее проведенного контроля;
– результаты мониторинга информационной безопасности;
– результаты выявления уязвимостей и инцидентов информационной безопасности.

6. МЕТОДЫ КОНТРОЛЯ УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ

6.1. Контроль уровня защищенности информации осуществляется с применением методов, достаточных для оценки фактического состояния защищенности информации и проверки корректности реализации мер защиты информации.

6.2. В ходе контроля могут применяться:
– анализ организационной и эксплуатационной документации;
– анализ состава и конфигурации ИС;
– анализ реализованных организационных и технических мер защиты информации;
– анализ настроек средств защиты информации;
– анализ журналов регистрации событий безопасности;
– анализ конфигураций программных и программно-аппаратных средств;
– анализ обновлений и сведений об уязвимостях;
– тестирование системы защиты информации;
– проверка корректности разграничения доступа;
– проверка корректности идентификации и аутентификации;
– проверка корректности регистрации событий безопасности;
– иные методы, применимые к конкретной ИС.

6.3. Конкретный состав методов контроля определяется работниками, ответственными за ИБ, с учетом архитектуры ИС, состава обрабатываемой информации, характера актуальных угроз, применяемых средств защиты информации и особенностей функционирования ИС.

6.4. При проведении контроля должны использоваться методы, не создающие недопустимых рисков нарушения работоспособности ИС, утраты данных либо нарушения штатного функционирования критически значимых компонентов.

7. ПРОВЕДЕНИЕ КОНТРОЛЯ УРОВНЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ

7.1. Контроль уровня защищенности информации проводится поэтапно и должен обеспечивать получение достаточных сведений для вывода о фактическом состоянии защиты информации в ИС.

7.2. В ходе контроля, как правило, выполняются:
– определение состава проверяемой ИС либо ее сегмента;
– определение целей и методов контроля;
– сбор исходных данных о конфигурации и функционировании ИС;
– анализ организационных и технических мер защиты информации;
– анализ защищенности ИС;
– тестирование системы защиты информации;
– фиксация выявленных недостатков и уязвимостей;
– оценка влияния выявленных недостатков на уровень защищенности информации;
– подготовка выводов и предложений.

7.3. При анализе защищенности ИС устанавливаются, в том числе:
– полнота реализации предусмотренных мер защиты информации;
– корректность настроек безопасности;
– наличие избыточных либо несанкционированных прав доступа;
– наличие уязвимостей и иных недостатков;
– соблюдение требований локальных нормативных актов Учреждения;

– наличие факторов, способных привести к нарушению конфиденциальности, целостности или доступности информации.

7.4. При тестировании системы защиты информации проверяется способность реализованных мер защиты обеспечивать требуемый уровень защищенности информации в реальных условиях эксплуатации ИС.

7.5. При проведении контроля в ИСПДн дополнительно учитываются:

– ранее установленный уровень защищенности персональных данных;

– тип актуальных угроз безопасности персональных данных;

– состав и содержание мер по обеспечению безопасности персональных данных, реализованных в ИСПДн;

8. ОЦЕНКА РЕЗУЛЬТАТОВ КОНТРОЛЯ

8.1. По результатам проведения контроля уровня защищенности информации должно быть установлено:

– соответствует ли фактическое состояние защиты информации установленным требованиям;

– обеспечивается ли достаточный уровень защищенности информации;

– имеются ли недостатки, способные привести к реализации актуальных угроз безопасности информации;

– требуется ли доработка, модернизация либо усиление системы защиты информации;

– требуется ли принятие компенсирующих мер.

8.2. Выявленные по результатам контроля недостатки подлежат анализу с точки зрения их влияния на безопасность информации, вероятность реализации угроз и возможные последствия для функционирования ИС.

8.3. При необходимости по результатам контроля подготавливаются предложения:

– по устранению выявленных недостатков;

– по изменению конфигурации ИС;

– по изменению порядка предоставления доступа;

– по применению дополнительных средств защиты информации;

– по корректировке локальных нормативных актов Учреждения;

– по выделению ресурсов для повышения уровня защищенности информации.

9. ОФОРМЛЕНИЕ РЕЗУЛЬТАТОВ КОНТРОЛЯ

9.1. По результатам проведения контроля уровня защищенности информации оформляется отчет по результатам контроля уровня защищенности информации, который подписывается лицами, проводившими контроль.

9.2. Отчет по результатам контроля уровня защищенности информации должен содержать:

– сведения о проверяемой ИС либо ее части;

– основание проведения контроля;

– примененные методы контроля;

– сведения о выявленных недостатках и уязвимостях;

– результаты анализа защищенности;

– результаты тестирования системы защиты информации;

– вывод о состоянии защищенности информации;

– предложения по повышению уровня защищенности информации и устранению выявленных недостатков.

9.3. Отчет должен быть представлен директору Учреждения либо ответственному лицу в течение 3 рабочих дней с даты завершения контроля уровня защищенности информации.

9.4. Отчет направляется Учреждением в ФСТЭК России в течение 5 рабочих дней с даты завершения контроля уровня защищенности информации.

9.5. Форма отчета по результатам контроля уровня защищенности информации, содержащейся в информационных системах представлена в приложении № 1 к настоящему Порядку.

10. СООТНОШЕНИЕ С ДОКУМЕНТАМИ ПО ИСПДН

10.1. Для ИСПДн, эксплуатируемых Учреждением, акт определения уровня защищенности персональных данных, оформляемый в соответствии с постановлением Правительства Российской Федерации от 01.11.2012 №1119, является самостоятельным документом, определяющим исходные условия защиты персональных данных.

10.2. Указанный акт не заменяет отчет по результатам контроля уровня защищенности информации, предусмотренный настоящим Порядком.

10.3. Форма акта определения уровня защищенности персональных данных в информационной системе персональных данных представлен в приложении № 2 к настоящему Порядку.

10.4. При проведении контроля уровня защищенности информации в ИСПДн сведения, содержащиеся в акте определения уровня защищенности персональных данных, используются как исходные данные для оценки фактического состояния защиты информации.

11. ОТВЕТСТВЕННОСТЬ

11.1. Работники, ответственные за ИБ, несут ответственность за организацию контроля уровня защищенности информации, выбор методов контроля, анализ результатов и подготовку отчета в пределах своей компетенции.

11.2. Работники, ответственные за эксплуатацию, несут ответственность за предоставление необходимых сведений о функционировании ИС, участие в проведении контроля и выполнение мероприятий по устранению выявленных недостатков в пределах своей компетенции.

11.3. Руководители структурных подразделений Учреждения несут ответственность за организацию выполнения мероприятий, предусмотренных настоящим Порядком, в пределах своей компетенции.

12. ПОРЯДОК ПЕРЕСМОТРА

12.1. Настоящий Порядок подлежит пересмотру при изменении законодательства Российской Федерации, обязательных требований в области защиты информации, локальных нормативных актов Учреждения, состава и архитектуры ИС, а также по результатам контроля, мониторинга информационной безопасности, расследования компьютерных инцидентов и аудитов.

12.2. Плановый пересмотр настоящего Порядка осуществляется не реже одного раза в 3 года.

12.3. Подготовку предложений по актуализации настоящего Порядка организуют работники, ответственные за ИБ.

Приложение № 1
к Порядку контроля уровня защищенности информации,
содержащейся в информационных системах

Форма отчета по результатам контроля уровня защищенности информации, содержащейся в информационных системах

ОТЧЕТ № ____
по результатам контроля уровня защищенности информации, содержащейся в информационной системе

_____

(наименование ИС)

1. Основание проведения контроля
Контроль уровня защищенности информации проведен на основании:
2. Состав комиссии
Комиссия в составе:
Председатель комиссии:
(должность, Ф.И.О.)
Члены комиссии:
(должность, Ф.И.О.)
3. Сведения об ИС
Наименование ИС:
Назначение ИС:
Категория ИС:
☐ федеральная
☐ государственная
☐ объектовая
☐ ИСПДн
☐ иная: _____
Место эксплуатации:
4. Исходные данные, учтенные при проведении контроля
В ходе контроля были учтены:
состав и структура ИС;
состав обрабатываемой информации;
архитектура ИС и состав применяемых средств защиты информации;
действующие локальные нормативные акты Учреждения;
сведения о ранее выявленных уязвимостях и инцидентах информационной безопасности;
сведения о ранее проведенных контрольных мероприятиях.
Для ИСПДн дополнительно учитывались:
установленный уровень защищенности персональных данных;
тип актуальных угроз безопасности персональных данных;
состав и содержание реализованных мер защиты персональных данных.
5. Примененные методы контроля
В ходе контроля применялись следующие методы:
☐ анализ организационной документации
☐ анализ эксплуатационной документации
☐ анализ конфигурации ИС
☐ анализ настроек средств защиты информации

☐ анализ журналов регистрации событий
☐ анализ обновлений
☐ анализ сведений об уязвимостях
☐ тестирование системы защиты информации
☐ проверка разграничения доступа
☐ проверка идентификации и аутентификации
☐ иные методы: _____

6. Результаты анализа защищенности

По результатам анализа защищенности установлено:
Выявленные недостатки и уязвимости:

7. Результаты тестирования системы защиты информации

В ходе тестирования системы защиты информации установлено:

8. Выводы комиссии

По результатам контроля комиссия пришла к следующим выводам:
☐ уровень защищенности информации является достаточным
☐ уровень защищенности информации требует повышения
☐ выявленные недостатки не препятствуют эксплуатации ИС
☐ выявленные недостатки требуют устранения до продолжения штатной эксплуатации
☐ требуется проведение дополнительных мероприятий по защите информации
Итоговый вывод:

9. Предложения комиссии

Комиссия предлагает:

10. Подписи лиц, проводивших контроль

Председатель комиссии
_____ /_____/

Члены комиссии
_____ /_____/

Приложение № 2
к Порядку контроля уровня защищенности информации,
содержащейся в информационных системах

Форма акта определения уровня защищенности персональных данных в информационных системах персональных данных

АКТ № ___

ОПРЕДЕЛЕНИЯ УРОВНЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ
ПРИ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ
ПЕРСОНАЛЬНЫХ ДАННЫХ

_____

(наименование ИС)

Комиссия в составе:

Председатель комиссии:
(должность, Ф.И.О.)
Члены комиссии:
(должность, Ф.И.О.)

Руководствуясь постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» в ходе обследования информационной системы персональных данных _____, (далее ИСПДн), комиссия выявила и определила следующие исходные данные, необходимые для установления уровня защищенности персональных данных при их обработке в ИСПДн:

1. Категория обработки персональных данных

В ИСПДн обрабатываются _____ категории персональных данных, т.к. _____

2. Объем обрабатываемых персональных данных

В ИСПДн осуществляется обработка данных менее/более чем 100 000 субъектов персональных данных, не являющихся/являющихся сотрудниками оператора.

3. Тип актуальных угроз безопасности

С учетом оценки возможного вреда, который может быть применен субъекту персональных данных в случае нарушений требований Федерального закона «О персональных данных», для ИСПДн устанавливаются актуальными угрозы безопасности данных ____ типа, _____

Заключение комиссии:

По результатам анализа данных в соответствии с требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 №1119, установить необходимость обеспечения _____ уровня защищенности персональных данных при их обработке в ИСПДн _____.

Подписи лиц, проводивших контроль

Председатель комиссии
_____ /_____/

Члены комиссии
_____ /_____/